D-Link DWS-3024L/3026
DWL-3500AP/8500AP
Unified Wired & Wireless Access System

ユーザマニュアル

ご注意

本書は、各製品ごとの機能の説明および設定方法を記載しています。本シリーズの仕様、設置方法など使用するために必要な基本的な取り扱い方法については、設置マニュアルをご覧ください。

D-Link®
Building Networks for People

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠警告	この表示を無視し、まちがった使いかたをすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、まちがった使いかたをすると、傷害または物損損害が発生するおそれがあります。

記号の意味　⃠ してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠警告

分解禁止
分解・改造をしない
機器が故障したり、異物が混入すると、やけどや火災の原因となります。

禁止
落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない
故障の原因につながります。

禁止
発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
感電、火災の原因になります。
使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼してください。

ぬれ手禁止
ぬれた手でさわらない
感電のおそれがあります。

水ぬれ禁止
水をかけたり、ぬらしたりしない
内部に水が入ると、火災、感電、または故障のおそれがあります。

禁止
油煙、湯気、湿気、ほこりの多い場所、振動の激しいところでは使わない
火災、感電、または故障のおそれがあります。

禁止
内部に金属物や燃えやすいものを入れない
火災、感電、または故障のおそれがあります。

禁止
表示以外の電圧で使用しない
火災、感電、または故障のおそれがあります。

禁止
たこ足配線禁止
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

禁止
設置、移動のときは電源プラグを抜く
火災、感電、または故障のおそれがあります。

禁止
雷鳴が聞こえたら、ケーブル / コード類にはさわらない
感電のおそれがあります。

禁止
ケーブル / コード類や端子を破損させない
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障につながります。

禁止
正しい電源ケーブル、コンセントを使用する
火災、感電、または故障の原因となります。

禁止
乳幼児の手の届く場所では使わない
やけど、ケガ、または感電の原因になります。

禁止
次のような場所では保管、使用をしない
・直射日光のあたる場所
・高温になる場所
・動作環境範囲外

禁止
光源をのぞかない
光ファイバケーブルの断面、コネクタ、および製品のコネクタをのぞきますと強力な光源により目を損傷するおそれがあります。

⚠注意

❗
静電気注意
コネクタやプラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。

❗
コードを持って抜かない
コードを無理に曲げたり、引っ張りますと、コードや機器の破損の原因となります。

❗
振動が発生する場所では使用しない
接触不良や動作不良の原因となります。

禁止
付属品の使用は取扱説明書にしたがう
付属品は取扱説明書にしたがい、他の製品には使用しないでください。機器の破損の原因になります。

電波障害自主規制について

DWS-3024L/3026 は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。
この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。
この場合には使用者が適切な対策を講ずるよう要求されることがあります。

DWL-3500AP/8500AP は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
本書の記載に従って正しい取り扱いをしてください。

無線に関するご注意

電波に関するご注意

DWL-3500AP/8500AP は、電波法に基づく小電力データ通信システムの無線製品として、技術基準適合証明を受けています。従って、本製品の使用する上で、無線局の免許は必要ありません。
本製品は、日本国内でのみ使用できます。
以下の注意をよくお読みになりご使用ください。

◎ この機器を以下の場所では使用しないでください。
- 心臓ペースメーカー等の産業・科学・医療用機器の近くで使用すると電磁妨害を及ぼし、生命の危険があります。
- 工場の製造ライン等で使用されている移動体識別用の構内無線局(免許を必要とする無線局)および特定小電力無線局(免許を必要としない無線局)
- 電子レンジの近くで使用すると、電子レンジによって無線通信に電磁妨害が発生します。

◎ 本製品は技術基準適合証明を受けています。本製品の分解、改造、および裏面の製品ラベルをはがさないでください。

5GHz 帯使用の無線機器に関するご注意

◎ 電波法により、5GHz 帯 (IEEE 802.11a) は屋外での使用が禁止されています。
◎ 従来の中心周波数（J52）を使用した機器とは通信チャンネルが異なるために通信できません。
◎ 802.11a（W53）使用時は気象レーダー等との電波干渉を避けるためにチャンネルを 自動的に変更する場合があります（DFS 機能）

2.4GHz 帯使用の無線機器の電波干渉に関するご注意

DWL-3500AP/8500AP の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用している移動体識別用の構内無線局 (免許を必要とする無線局) および特定小電力無線局 (免許を必要としない無線局) 並びにアマチュア無線局 (免許を必要とする無線局) が運用されています。

◎ この機器を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。
◎ 万一、この機器から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止してください。
◎ その他、この機器から移動体通信用の特定小電力無線局に対して電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、弊社サポート窓口へお問い合わせください。

使用周波数帯域	2.4GHz 帯
変調方式	DS-SS 方式 /OFDM 方式
想定干渉距離	40m 以下
周波数変更可否	全帯域を使用し、かつ移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局の帯域を回避可能

無線 LAN 製品ご使用時におけるセキュリティに関するご注意

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

◎ 通信内容を盗み見られる
悪意ある第三者が、電波を故意に傍受し、以下の通信内容を盗み見られる可能性があります。
- ID やパスワード又はクレジットカード番号等の個人情報
- メールの内容

◎ 不正に侵入される
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、以下の行為を行う可能性があります。
- 個人情報や機密情報を取り出す（情報漏洩）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き換えて発信する（改ざん）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- 保守マーク表示を守ってください。また、ドキュメント類に説明されている以外の方法でのご使用はやめてください。三角形の中に稲妻マークがついたカバー類をあけたり外したりすると、感電の危険性を招きます。筐体の内部は、訓練を受けた保守技術員が取り扱うようにしてください。
- 以下のような状況に陥った場合は、電源ケーブルをコンセントから抜いて、部品の交換をするかサービス会社に連絡してください。
  - 電源ケーブル、延長ケーブル、またはプラグが破損した。
  - 製品の中に異物が入った。
  - 製品に水がかかった。
  - 製品が落下した、または損傷を受けた。
  - 操作方法に従って運用しているのに正しく動作しない。
- 本製品をラジエータや熱源の近くに置かないでください。また冷却用通気孔を塞がないようにしてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。万一製品が濡れてしまった場合は、トラブルシューティングガイドの該当する文をお読みになるか、サービス会社に連絡してください。
- 本システムの開口部に物を差し込まないでください。内部コンポーネントのショートによる火事や感電を引き起こすことがあります。
- 本製品と一緒にその他のデバイスを使用する場合は、弊社の認定を受けたデバイスを使用してください。
- カバーを外す際、あるいは内部コンポーネントに触れる際は、製品の温度が十分に下がってから行ってください。
- 電気定格ラベル標記と合致したタイプの外部電源を使用してください。正しい外部電源タイプが分からない場合は、サービス会社、あるいはお近くの電力会社にお問い合わせください。
- システムの損傷を防ぐために、電源装置の電圧選択スイッチ（装備されている場合のみ）がご利用の地域の設定と合致しているか確認してください。
  - 東日本では 100V/50Hz、西日本では 100V/60Hz
- また、付属するデバイスが、ご使用になる地域の電気定格に合致しているか確認してください。
- 付属の電源ケーブルのみを使用してください。
- 感電を防止するために、本システムと周辺装置の電源ケーブルは、正しく接地された電気コンセントに接続してください。このケーブルには、正しく接地されるように、3 ピンプラグが取り付けられています。アダプタプラグを使用したり、ケーブルから接地ピンを取り外したりしないでください。延長コードを使用する必要がある場合は、正しく接地されたプラグが付いている 3 線式コードを使用してください。
- 延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動からシステムコンポーネントを保護するには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏み付けられたりつまずいたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルやプラグを改造しないでください。設置場所の変更をする場合は、資格を持った電気技術者または電力会社にお問い合わせください。国または地方自治体の配線規則に必ず従ってください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いてください。
- 製品の移動は気をつけて行ってください。キャスタやスタビライザがしっかり装着されているか確認してください。急停止や、凹凸面上の移動は避けてください。

ラック搭載型製品に関する一般的な注意事項

ラックの安定性および安全性に関する以下の注意事項を遵守してください。また、システムおよびラックに付随する、ラック設置マニュアル中の注意事項や手順についてもよくお読みください。

警告 前面および側面のスタビライザを装着せずに、システムをラックに搭載すると、ラックが倒れ、人身事故を引き起こす場合があります。ラックにシステムを搭載する前には、必ずスタビライザを装着してください。

警告 接地用伝導体を壊したり、接地用伝導体を適切に取り付けないで装置を操作しないでください。適切な接地ができるかわからない場合、電気保安協会または電気工事士にお問い合わせください。

警告 システムのシャーシは、ラックキャビネットのフレームにしっかり接地される必要があります。接地ケーブルを接続してから、システムに電源を接続してください。電源および安全用接地配線が完了したら、資格を持つ電気検査技師が検査する必要があります。安全用接地ケーブルを配線しなかったり、接続されていない場合、エネルギーハザードが起こります。

- システムとは、ラックに搭載されるコンポーネントを指しています。コンポーネントはシステムや各種周辺デバイスや付属するハードウェアも含みます。
- ラックにシステム / コンポーネントを搭載した後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは 1 つのみとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。
- ラックに装置を搭載する前に、スタビライザがしっかりとラックに固定されているか、床面まで到達しているか、ラック全体の重量がすべて床にかかるようになっているかをよく確認してください。ラックに搭載する前に、シングルラックには前面および側面のスタビライザを、複数結合型のラックには前面用スタビライザを装着してください。
- ラックへの装置の搭載は、常に下から上へ、また最も重いものから行ってください。
- ラックからコンポーネントを引き出す際には、ラックが水平で、安定しているかどうか確認してから行ってください。
- コンポーネントレール解除ラッチを押して、ラックから、またはラックへコンポーネントをスライドさせる際は、指をスライドレールに挟まないよう、気をつけて行ってください。
- ラックに電源を供給する AC 電源分岐回路に過剰な負荷をかけないでください。ラックの合計負荷が、分岐回路の定格の 80 パーセントを超えないようにしてください。
- ラック内部のコンポーネントに適切な空気流があることを確認してください。
- ラック内の他のシステムを保守する際には、システムやコンポーネントを踏みつけたり、その上に立ったりしないでください。

注意 資格を持つ電気工事士が、DC 電源への接続と接地を行う必要があります。すべての電気配線が、お住まいの地域、および国の電気基準と規制に準拠していることを確認してください。

静電気障害を防止するために

静電気は、システム内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、マイクロプロセッサなどの電子部品に触れる前に、身体から静電気を逃がしてください。シャーシの塗装されていない金属面に定期的に触れることにより、身体の静電気を逃がすことができます。

さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 静電気に敏感なコンポーネントを箱から取り出す時は、コンポーネントをシステムに取り付ける準備が完了するまで、コンポーネントを静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃してください。
2. 静電気に敏感な部品を運ぶ場合、最初に静電気防止容器またはパッケージに入れてください。
3. 静電気に敏感なコンポーネントの取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

バッテリの取り扱いについて

警告 不適切なバッテリの使用により、爆発などの危険性が生じることがあります。バッテリの交換は、必ず同じものか、製造者が推奨する同等の仕様のものをご使用ください。バッテリの廃棄については、製造者の指示に従って行ってください。

電源の異常について

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。
電源が再度供給できる状態になってから電源プラグを再度接続します。

安全にお使いいただくために

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および同梱されている製品保証書をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

- 本書および同梱されている製品保証書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 本書および同梱されている製品保証書は大切に保管してください。
- 弊社製品を日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
また、テクニカルサポートご提供のためにはユーザ登録が必要となります。
http://www.dlink-jp.com/

目次

安全にお使いいただくために 2
ラック搭載型製品に関する一般的な注意事項 4
静電気障害を防止するために 5
バッテリの取り扱いについて 5
電源の異常について 5

まえがき 9

本マニュアルの対象 9
本マニュアルの構成 9
本マニュアル中の表記方法について 9

第 1 章　はじめに 10

1.1 D-Link 統合アクセスシステムのコンポーネント 10
1.2 D-Link 統合アクセスシステムのトポロジ 11
1.3 ユーザインタフェースについて 12
1.4 サポートする機能 17

第 2 章　D-Link 統合アクセスシステム・ネットワークの設計 18

2.1 システム要件 18
2.2 WLAN トポロジについて 19
2.3 レイヤ 3 ローミング実現のためのネットワーク設計 21

第 3 章　ハードウェアの設置 22

3.1 ハードウェアの概要 22
3.2 設置 24
3.3 スイッチの接続 28

第 4 章　D-Link 統合アクセスシステムの設定 30

4.1 システムの設置について 30
4.2 スイッチのネットワークへの接続 31
4.3 スイッチの WLAN 機能の有効化 33
4.4 アクセスポイント側の準備 34
4.5 アクセスポイントとピアスイッチの検出 36
4.6 アクセスポイントの認証 48

第 5 章　アクセスポイントの設定 54

5.1 アクセスポイントプロファイル、ネットワーク、ローカルデータベース 54
5.2 AAA と RADIUS の設定 55
5.3 無線電波の設定 57
5.4 SSID の設定 61
5.5 Valid アクセスポイントの設定 69

第 6 章　D-Link アクセスポイントの保守管理 71

6.1 アクセスポイントの再起動 71
6.2 無線周波数帯の管理 71
6.3 アクセスポイントソフトウェアの更新 75
6.4 高度なアクセスポイント管理 77

第 7 章　状態および統計情報のモニタ 80

7.1 無線グローバル情報のモニタ 80
7.2 ピアスイッチの状態モニタ 82
7.3 全アクセスポイントのモニタ 83
7.4 管理対象アクセスポイントの状態モニタ 84
7.5 アクセスポイントの認証失敗状況の参照 96
7.6 不正アクセスポイントのモニタとアクセスポイントの RF スキャン 97
7.7 接続中のクライアントのモニタ 99
7.8 クライアントの認証失敗状況の参照 105
7.9 アドホッククライアントのモニタと管理 106

第 8 章　システムの詳細設定 108

8.1 アクセスポイントプロファイルの作成、設定、管理 108
8.2 グローバル設定 111
8.3 SNMP トラップの有効化 112
8.4 QoS の設定 113

第 9 章　キャプティブポータル設定 115

9.1 グローバルキャプティブポータル設定 115
9.2 キャプティブポータルの設定 116
9.3 キャプティブポータルユーザのモニタと設定 120
9.4 インタフェースへのキャプティブポータルの割り当て 122
9.5 キャプティブポータルステータスの参照 123
9.6 クライアントサマリの参照 126
9.7 SNMP トラップ設定 129

第 10 章　無線ネットワークの視覚化 130

10.1 背景画像のインポートと設定 131
10.2 グラフコンポーネントの設定 131
10.3 メニューバーについて 134
10.4 グラフの管理 136

付録 A　D-Link 統合アクセスシステムの初期設定 138

A.1 DWS-3026 の初期設定 138
A.2 D-Link アクセスポイントプロファイルの初期設定 139
A.3 キャプティブポータル設定の初期値 140

付録 B　外部 RADIUS サーバの設定 141

B.1 RADIUS サーバでのアクセスポイント設定 141
B.2 FreeRADIUS を使用した RADIUS サーバ設定例 142
B.3 RADIUS サーバでの無線クライアント設定 144
B.4 FreeRADIUS を使用した無線クライアント設定例 144

付録 C　L3 ローミング設定例 146

C.1 WLAN とトンネルインタフェースの設定 146
C.2 L3 トンネルネットワークの設定 151
C.3 DHCP リレーと DHCP サーバの設定 155

付録 D　QoS 制御について 157

QoS とロードバランシング 157
802.11e と WMM 標準のサポート 157
トラフィックフローの調整 157
QoS キューとパケット内の DSCP 157
データフレームの EDCF 制御と AIFS 158
ランダムバックオフとコンテンション画面 158
性能向上のためのパケットバースティング機能 159
クライアントの TXOP インターバル 159
IEEE 802.1p 標準と DSCP タグ 159

まえがき

本マニュアルでは、D-Link 統合アクセスシステムのご利用にあたり、ネットワーク設計、設定、および保守運用について記述するものです。

本マニュアルの対象

本マニュアルは、ネットワークインフラストラクチャの一部としての D-Link 統合アクセスシステムの設置、設定、監視および運用をする方を対象としています。

本マニュアルの構成

D-Link 統合アクセスシステム・ユーザマニュアルは以下の章で構成されています。

第 1 章　はじめに

第 2 章　D-Link 統合アクセスシステム・ネットワークの設計

第 3 章　ハードウェアの設置

第 4 章　D-Link 統合アクセスシステムの設定

第 5 章　アクセスポイントの設定

第 6 章　D-Link アクセスポイントの保守管理

第 7 章　状態および統計情報のモニタ

第 8 章　システムの詳細設定

第 9 章　キャプティブポータルの設定

第 10 章　無線ネットワークの視覚化

付録 A　D-Link 統合アクセスシステムの初期設定

付録 B　外部 RADIUS サーバの設定

付録 C　L3 ローミング設定例

付録 D　QoS 制御について

本マニュアル中の表記方法について

本項では、本マニュアル中での表記方法について説明します。

注意　注意では、特長や技術についての詳細情報を記述します。

警告　警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	「まえがき」（13 ページ）をご参照ください。
`courier` フォント	CLI 出力文字、ファイル名。	`(switch-prompt)#`
`courier` 太字	コマンド、ユーザによるコマンドライン入力。	**`show network`**
`courier` 斜体	コマンドパラメータ（可変または固定）。	*`value`*
< >	可変パラメータ。< > にあたる箇所に値または文字を入力します。	<*`value`*>
[ ]	任意の固定パラメータ。	[*`value`*]
[< >]	任意の可変パラメータ。	[<*`value`*>]
{ }	{ } 内の選択肢から 1 つ選択して入力するパラメータ。	{*`choice1`* | *`choice2`*}
|（垂直線）	相互排他的なパラメータ。	*`choice1`* | *`choice2`*
[{ }]	任意のパラメータで、指定する場合はどちらかを選択します。	[{*`choice1`* | *`choice2`*}]

第 1 章　はじめに

D-Link 統合アクセスシステムは、最新鋭の無線ネットワーク機能を実現しながら WLAN（無線 LAN）の展開を可能にします。さらに確実な接続性と、シームレスなレイヤ 2 とレイヤ 3 ローミングをエンドユーザに提供する拡張可能なソリューションです。

本章は以下の項で構成されています。

- D-Link 統合アクセスシステムのコンポーネント
- D-Link 統合アクセスシステムのトポロジ
- ユーザインタフェースについて
- サポートする機能

1.1 D-Link 統合アクセスシステムのコンポーネント

D-Link 統合アクセスシステムのコンポーネントは D-Link 統合スイッチと D-Link アクセスポイント（AP）で構成されます。

DWS-3024L は最大 24 台、DWS-3026 スイッチは最大 48 台の D-Link アクセスポイントを管理することができます。
各管理アクセスポイントは最大 512 台までの無線クライアントと接続が可能です（各無線インタフェースにつき 256 台）。統合スイッチは配下にあるすべての WLAN のトラフィックとデバイスの状態および統計情報を追跡記録します。

最大 4 台までのピア統合スイッチを構成し、アクセスポイントと配下にある無線クライアントの様々な情報を共有することができます。ピア統合スイッチ同士は、直接接続したり、レイヤ 2 ブリッジにより分割したり、また異なる IP サブネットに所属することができます。この統合スイッチにより、無線クライアントは、AP 間をネットワークへの接続を保ったままローミングすることが可能となります。

D-Link 統合スイッチ

D-Link 統合スイッチは有線 LAN、無線 LAN の両方のトラフィックに対し、レイヤ 2, レイヤ 3, レイヤ 4 のスイッチングおよびルーティング機能を持っています。DWS-3024L は最大 24 台、DWS-3026 は最大 48 の台のアクセスポイント（AP）を管理することができます。統合スイッチのユーザインタフェースを使用して、ネットワーク内のすべてのアクセスポイントに対して設定、確認、およびデータの保守ができます。

統合スイッチは接続性の高いデータ経路の接続性、モビリティ制御、セキュリティ保護、無線・電力パラメータ制御、およびネットワークとネットワークエレメントの管理機能を提供します。また、不正 AP と不正クライアントの検出や状態を含むピア無線スイッチや D-Link アクセスポイント、また WLAN 上のクライアントの検出、確認、認証、および監視を行います。

D-Link 統合アクセスシステムでは以下のスイッチを使用できます。:

- DWS-3024L - ギガポートを 24 ポート、SFP ポートとのコンボポートを 4 ポートおよびリダンダント電源コネクタを装備しています。
- DWS-3026 - ギガポートを 24 ポート、SFP ポートとのコンボポートを 4 ポート、10 ギガアップリンク用拡張スロットを 2 スロットおよびリダンダント電源コネクタを装備しています。

D-Link アクセスポイント

D-Link アクセスポイントは、2 つのモード（スタンドアロンモードまたは管理モード）のいずれかで動作します。スタンドアロンモードでは、D-Link アクセスポイントはネットワークで個々のアクセスポイントとして動作するため、管理者は AP に接続して、Web ユーザインタフェース（UI）またはコマンドラインインタフェース（CLI）を使用することで管理します。管理モードでは、D-Link アクセスポイントは D-Link 統合アクセスシステムの一部となり、D-Link 統合スイッチを使用して管理を行います。アクセスポイントが管理モードの場合、アクセスポイントの管理者用 Web インタフェースは無効とされます。アクセスは Telnet を経由した CLI に制限されます。

スタンドアロンモードは 2、3 台のアクセスポイントを使用する小規模のネットワークに適しています。管理モードはどんな規模のネットワークにも使用できます。スタンドアロンモードで D-Link アクセスポイントの使用を開始しても、統合スイッチをネットワークに追加する際にその AP を管理モードに容易に移行することができます。管理モードでアクセスポイントを使用することにより、統合スイッチから配下のアクセスポイントに対しコンフィグレーションプロファイルの移行やソフトウェアアップグレードの指示が行われるため、アクセスポイント管理の集中化、アップグレードの効率化が実現できます。D-Link 統合アクセスシステムのユーザマニュアルでは、主に D-Lin 管理モードのと D-Link アクセスポイントについて記述しています。スタンドアロンモードにおける D-Link アクセスポイント設定に関する情報については、Unified Access Point（AP）Administrator' s Guide を参照してください。

D-Link 統合アクセスシステムは、以下の D-Link 製アクセスポイントと連携します。
- DWL-3500AP
- DWL-8500AP

DWL-3500AP は 1 つ、DWL-8500AP は 2 つの無線インタフェースをサポートします。DWL-3500AP と DWL-8500AP の 1 つの無線インタフェースは IEEE 802.11g モードで動作し、DWL-8500AP のもう 1 つの無線インタフェースは IEEE 802.11a モードで動作します。

各アクセスポイントは各無線インタフェースにつき、8 つまでの仮想アクセスポイント（VAP）をサポートします。VAP 機能により、各物理アクセスポイントを（無線インタフェースごとに）8 つの論理アクセスポイントに分割し、それぞれに異なる SSID、VLAN ID、およびセキュリティポリシーを持たせることができます。

WLAN の視覚化

D-Link 統合アクセスシステムが提供する WLAN 視覚化ツールを利用することにより、ユーザは Web ブラウザからご使用の無線ネットワークをグラフィカルに捉えることができます。WLAN 視覚化ツールは D-Link 統合スイッチ、D-Link アクセスポイント、他のアクセスポイントおよび D-Link アクセスポイントに接続する無線クライアントを検出し、表示することができます。

現場における建物のレイアウトなどの情報をインポートし、ネットワークビューとしてカスタマイズすることも可能です。

図 1-1 には、フロアプランと、D-Link 統合スイッチと配下の 2 台のアクセスポイントで構成するネットワークの例を示します。図には 1 組のピアスイッチと不正アクセスポイントも表示されています。

図 1-1　WLAN 視覚化の例

WLAN 視覚化ツールは、アクセスポイントの電波出力をチャンネルごとに色分けして表示するため、干渉を低減し、WLAN のカバー範囲を増強させるアクセスポイントの設置位置を決定する際などに非常に有効です。

1.2 D-Link 統合アクセスシステムのトポロジ

WLAN のネットワークトポロジは、ご使用のネットワークの規模および要求事項によって異なります。小規模から中規模のネットワークでは、1 台の統合スイッチで少数の D-Link アクセスポイントを管理することができます。大規模なネットワークでは、無線クライアントによるローミングの機能がさらに必要となり、複数のピアスイッチを導入し、それぞれがアクセスポイントを管理します。

1 台の統合スイッチの配置

D-Link アクセスポイントを設置すると、D-Link 統合スイッチは自動的にアクセスポイントを検出し、自動 RF チャンネル選択や自動出力調整などを含むデフォルトプロファイルを適用します。

図 1-2 は 1 台の統合スイッチが 3 台の D-Link アクセスポイントを管理するネットワーク構成を示します。

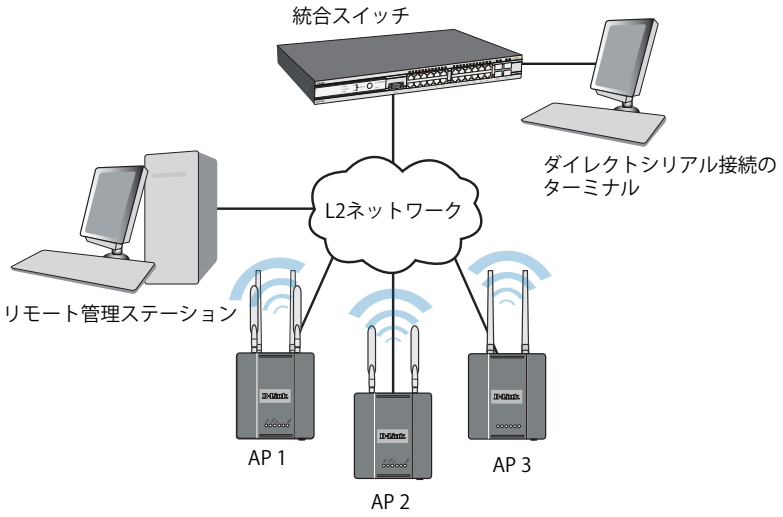


図 1-2　1 台の統合スイッチによるレイヤ 2 ローミングのサポート

アクセスポイントが同じサブネットに属し、同じ SSID を持つ場合、無線クライアントはそれらの全アクセスポイント間でローミングを行い、途切れることなくネットワークにアクセスすることができます。その際、クライアントは同じ IP アドレスを使用し、異なるアクセスポイントのブロードキャストエリアに入る時も再認証の必要はありません。アクセスポイント間のコンフィグレーション変更は、スイッチが同時に、またはアクセスポイントごとに行います。

ピア統合スイッチの配置

規模の大きいネットワークを構築するためには、4 台のスイッチをピアとしてネットワークを構成することで WLAN の規模と無線通信範囲を増強することができます。図 1-3 は、3 台のピアスイッチを配備した D-Link 統合アクセスシステムの構成例です。各ピアスイッチは最大 48 台（DWS-3026）または 24 台（DWS-3024L）のアクセスポイントを管理することができます。統合スイッチと管理下にあるアクセスポイントは、同じサブネット内である必要はありません。

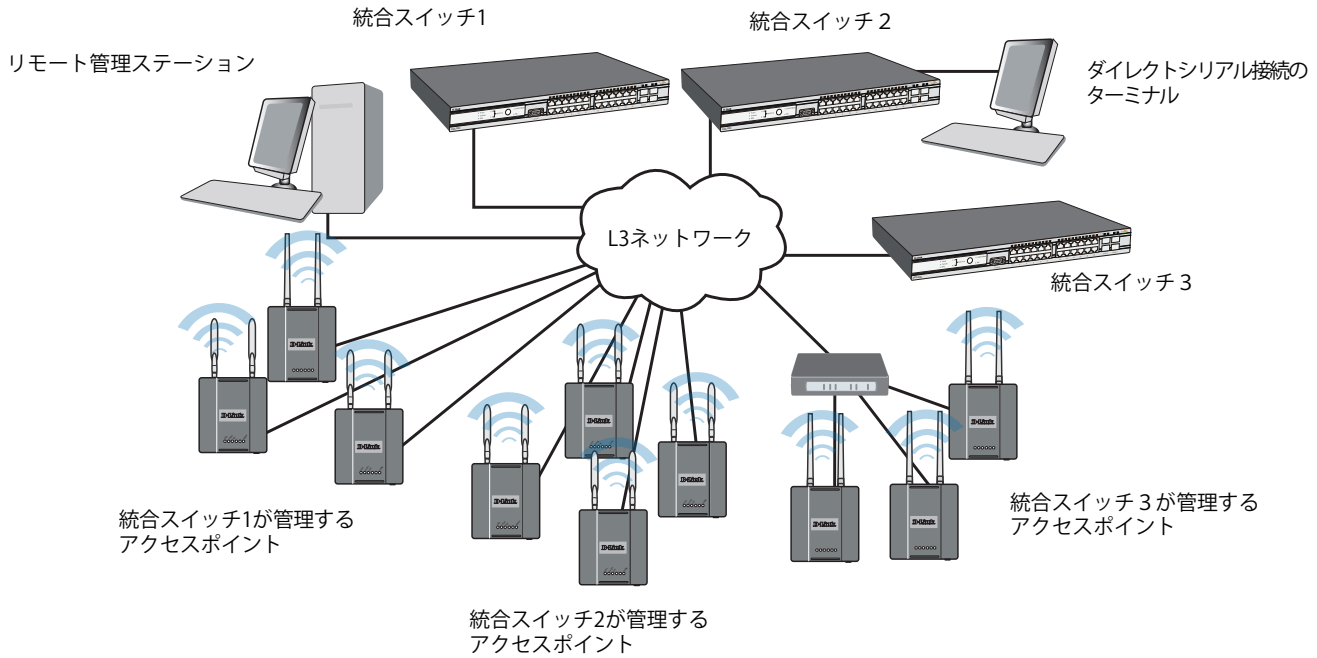


図 1-3　ピア統合スイッチによるレイヤ 3 ローミングのサポート

ピアスイッチ間でアクセスポイントの情報を共有し、アクセスポイントのスイッチ間を越えたレイヤ 3 ローミングを可能にします。これを実現するために、ピアスイッチは IPv4 トンネルを構築し、無線クライアントが異なるサブネットに存在するアクセスポイントに接続する際も、同じ IP アドレスを使えるようにします。レイヤ 3 ローミングサービスによって、無線電話の利用者も、異なるサブネットに属するアクセスポイント間を、途切れることなく行き来することができます。

1.3 ユーザインタフェースについて

D-Link 統合アクセスシステムは、複数のアクセスポイントの集中管理を行います。それにより、デバイスの配置、管理が容易になるばかりでなく、セキュリティの強化にもつながります。本システムでは、以下の 3 つの方法を使用して、WLAN の管理および監視を包括的に行います。

- Web ベース
- コマンドライン・インタフェース（CLI）
- 簡易ネットワーク管理プロトコル（SNMP）

上記の各管理方法は、D-Link 統合アクセスシステムの構成要素の設定、管理、および制御をローカルまたはリモートで行うことができます。本システムは標準的なコンフィグレーションパラメータやプライベート MIB と呼ばれるどの装置にも共通に定義されている MIB 以外もサポートします。本システムの設定および監視方法については、ネットワークの規模や、ご希望により選択してください。

Web インタフェースを使用する

Web ブラウザからスイッチにアクセスするためには、操作をする PC に以下のソフトウェアが必要です。

- Internet Explorer 6.0 以降

以下の手順で Web インタフェースにログインしてください。

1. Web ブラウザを起動し、「アドレス」欄にスイッチの IP アドレスを入力します。本スイッチの IP アドレスの初期値は「10.90.90.90」です。

図 1-4　アドレス入力

2. 表示されたダイアログボックスに、「User Name」（ユーザ名）および「Password」（パスワード）を入力し、「Login」ボタンをクリックします。

図 1-5　ログイン

参照　ユーザ名とパスワードはコマンドライン・インタフェースにログインする際に使用するものと同じです。初期値ではユーザ名が「admin」、パスワードは設定されていません。

3. システムから認証を受けると、「System Description」画面が表示されます。

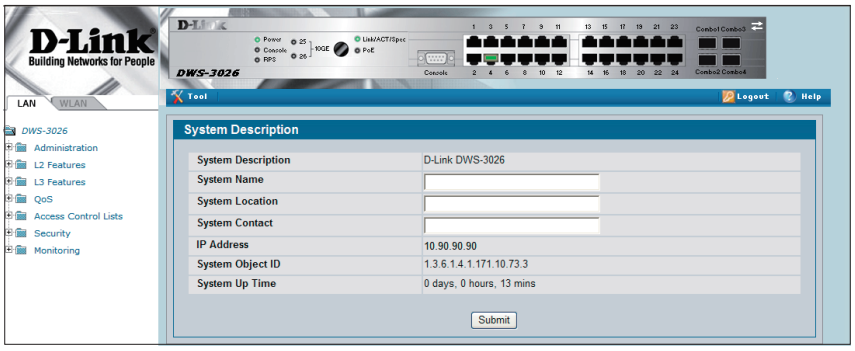


図 1-6　初期画面

図 1-7 に D-Link 統合スイッチの Web インタフェースのレイアウト例を示します。ページは「インタフェース構成図」、「ナビゲーションツリー」、「設定状況・オプション」の 3 つのメインエリアから構成されています。

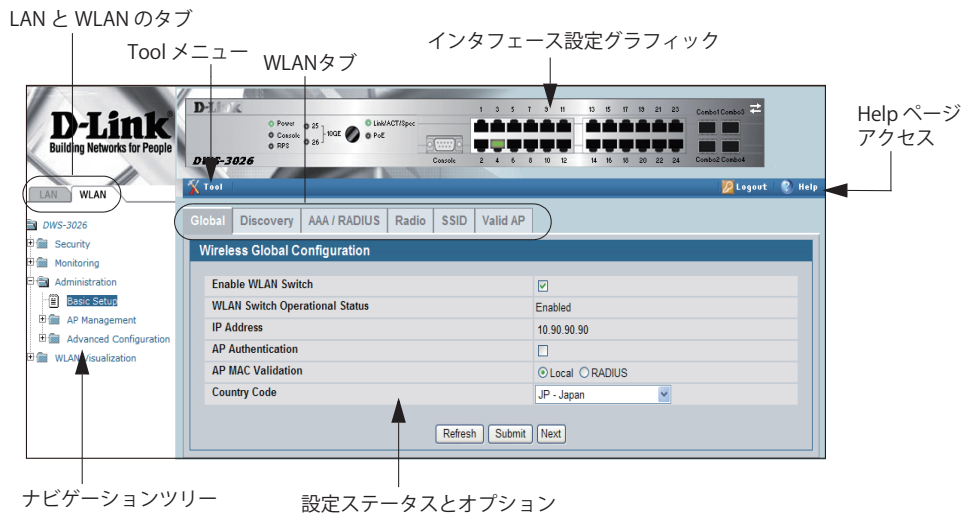


図 1-7　Web インタフェースのレイアウト

インタフェース構成図

「インタフェース構成図」は Java™ アプレットで、D-Link 統合スイッチ上のポートが図示されます。この図は各ページの上部に表示され、ここからも設定およびモニタリングオプションへと移行できるように設計されています。

確認や設定を行いたいポートをクリックすると、統計や設定オプションなどのメニューが表示されます。目的のメニューをクリックし、設定やモニタリングオプションをするページへと移行します。「Logout」ボタンをクリックし、スイッチの Web インタフェースからログアウトします。Logout プロンプトから、「OK」をクリックして、変更を保存して、適用します。変更を保存しない場合は「Cancel」をクリックして、Web インタフェースをクローズします。

グラフィック部分の、ポート以外の場所をクリックすると、メインメニューが表示されます。このメニューの内容は、ページ左側に表示される、ナビゲーションメニューと同じです。

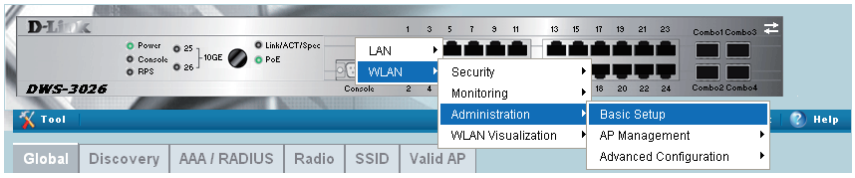


図 1-8　カスケード形式のナビゲーションメニュー

ナビゲーションメニュー

画面左側に階層型のツリー構造が表示されます。ツリー構造はフォルダ、サブフォルダ、および設定と状態表示をする HTML ページで構成されます。フォルダをクリックするとフォルダの内部が表示されます。各フォルダはサブフォルダまたは HTML ページ、またはその両方を格納しています。図 1-9 にナビゲーションメニュー内のフォルダ、サブフォルダ、HTML ページの例を示します。左側に「＋」マークのあるフォルダまたはサブフォルダをクリックすると、フォルダの内容が表示されます。HTML ページをクリックすると、メインフレーム内に新しいページが表示されます。フォルダやサブフォルダをクリックしても新しいページは表示されません。

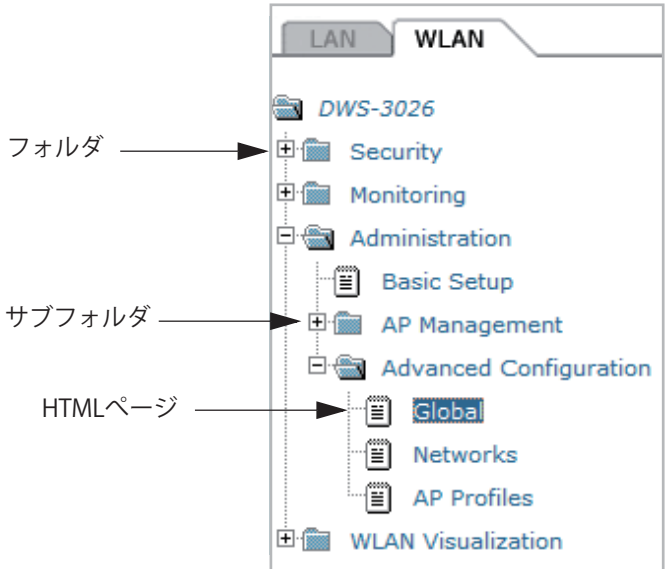


図 1-9　階層型ツリー構造のナビゲーションメニュー

設定・モニタリングオプション

画面中、インタフェース構成図の下、ナビゲーションメニューの右側には、選択したページの設定情報または現在の状況が表示されます。設定オプションが表示されるページでは、フィールド内に入力したり、プルダウンメニューを選択するなどの操作を行います。

各ページには HTML ベースのヘルプが用意されており、フィールドや設定オプションの詳細などを確認することができます。多くのページにはコマンドボタンも用意されています。

以下のコマンドボタンは、Web インタフェースのどのページにも表示されます。

項目	説明
Submit	更新した設定内容がスイッチに送信されます。設定の変更は直ちに行われますが、設定事項の中には電源をオフにすると失われてしまうものがあります。そのような設定は事前にシステムコンフィグレーションファイルに保存しておく必要があります。
Save	現在の設定内容をシステムコンフィグレーションファイルに保存します。このボタンを押すと、スイッチに送信した変更内容は、システムのリブートを行った後にも保存されます。設定の保存には「Tool」メニュー中の「Save Changes」を使用することもできます。
Refresh	画面上のデータを更新します。

「WLAN」タブ

WLAN フォルダのページには、操作を簡単にし、共通の機能をグループ化するためにタブが用意されています。タブをクリックして目的のページにアクセスします。

注意 ソフトウェアスイートのほかのパッケージでは、Web インタフェース中のタブはご利用できません。

ツールメニュー

「Tool」アイコンをマウスでポイントすると、以下の便利なシステムツールが表示されます。

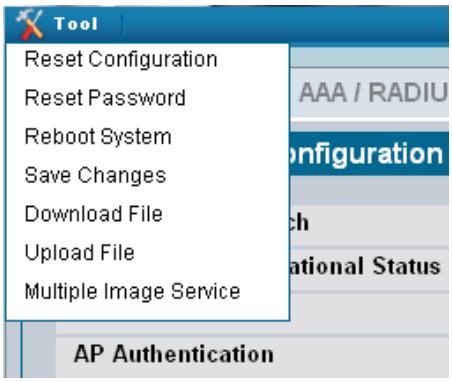


図 1-10　ツールメニュー

項目	説明
Reset Configuration	工場出荷時設定に戻します。
Reset Password	パスワードをリセットします。
Reboot System	本製品をリブートします。
Save Changes	設定を本製品に保存します。
Download File	設定内容のバックアップをします。
Upload File	設定内容をリストアします。
Multiple Image Service	設定ファイルを変更します。

リスト表示されている各ツールをクリックすると、それぞれの操作をする Web ページに移動します。

コマンドライン・インタフェースを使用する

コマンドライン・インタフェース（CLI）とは、テキストベースのコマンドを入力することにより、システムの管理と監視をする方法です。CLI はダイレクトシリアル接続、または Telnet や SSH にてリモートから論理接続して行うことができます。

CLI では、コマンドを機能によってモードで分類しています。コマンドモードによりサポートするコマンドが異なります。つまり、あるコマンドは、ある特定のモードに遷移した状態でないと実行することができません。ただし、User EXEC モードのコマンドはすべて Privilege EXEC モードで実行することができます。

現在のモードで使用可能なコマンドを確認するためには、コマンドプロンプトの後に、クエスチョンマーク「?」を入力します。使用可能なコマンドのキーワードやパラメータを確認するためには、コマンドプロンプトの後にタイプしたテキストの後に、クエスチョンマーク「?」を入力します。追加するコマンドキーワードやパラメータがない場合、または追加のパラメータが任意である場合、以下のメッセージが表示されます。

```
<cr>            Press Enter to execute the command
```

CLI についての詳細は、本製品付属の CD-ROM に収録の「D-Link CLI MANUAL」をご参照ください。

「D-Link CLI MANUAL」には CLI で使用するコマンドがリスト形式で掲載されています。リストには、コマンド名ごとの簡単な説明と以下の情報が記されています。

- コマンドキーワードと必須および任意のパラメータ
- コマンドを実行するモード
- 初期値（設定されている場合）

show コマンドで表示する情報の内容は、「D-Link CLI MANUAL」中の show コマンドのページで参照することができます。

SNMP を使用する

D-Link 統合スイッチのソフトウェアは SNMP モジュールを実装し、SNMP グループやユーザの設定を行い、SNMP エージェントが送信するトラップの管理をすることができます。

D-Link 統合スイッチは、標準的な機能をカバーするパブリック MIB と、さらにスイッチが提供する追加機能を実現させるプライベート MIB の両方をサポートしています。すべてのプライベート MIB はプレフィックス「DLINK-」で始まります。インタフェースコンフィグレーションのメインオブジェクトはプライベート MIB である、「DLINK-SWITCHING-MIB」に存在します。パブリック MIB や IF-MIB のオブジェクトにもインタフェースコンフィグレーションは含まれます。

SNMP は初期状態で有効になっています。スイッチにアクセスする SNMP マネージャの設定をするために必要な情報は、Web インタフェースにログインすると最初に表示される「System Description」画面と、「`show sysinfo`」コマンドで参照することができます。

すべてのユーザは SNMPv3 プロトコルを利用してスイッチに接続することができます。しかし、認証および暗号化の設定のために、新規にユーザプロファイルの作成をする必要があります。CLI を使用してプロファイルを作成するためには、「D-Link CLI MANUAL」の SNMP の項を参照してください。Web インタフェースを用いる場合には、以下の手順に従い行ってください。

新規にユーザプロファイルの作成をする

1. Web インタフェースの左側に表示されるツリー構造から、**LAN > Administration > User Accounts** の順に選択します。

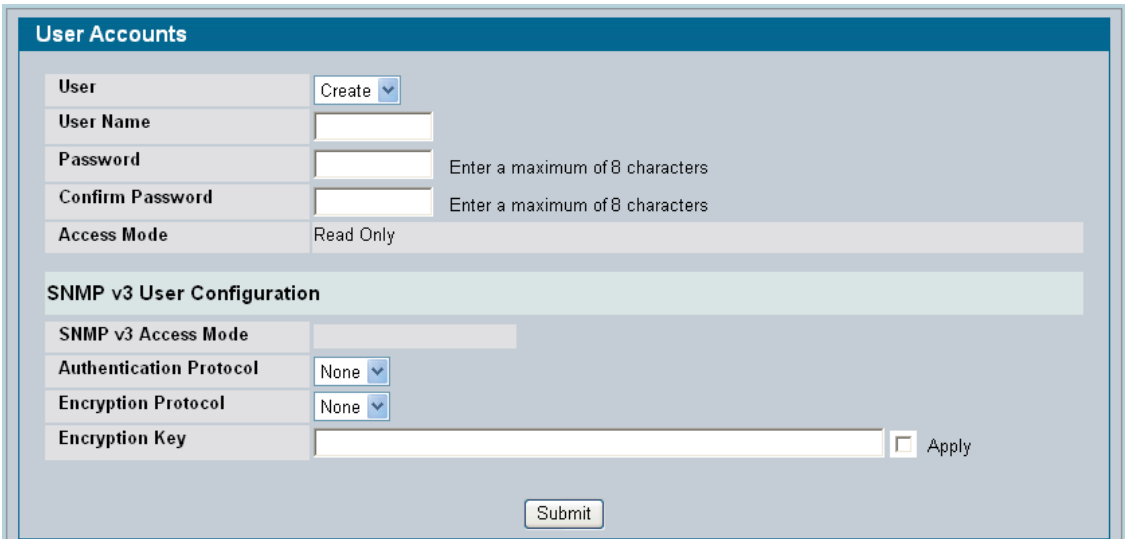


図 1-11　User Accounts 画面

2. 「User」プルダウンメニューから「Create」を選択し、新規ユーザを登録します。

3. 「User Name」欄にユーザ名を入力します。

4. 「Password」欄にパスワードを入力し、「Confirm Password」欄にも再度入力します。

注意 SNMPv3 認証を使用するためには、パスワードとして半角英数字 8 文字以上を入力します。

5. 認証を有効にするためには、「Authentication Protocol」プルダウンメニューから認証プロトコルとして「MD5」または「SHA」を選択します。

6. 暗号化を有効にするためには、「Encryption Protocol」プルダウンメニューから、暗号スキーム「DES」を選択します。さらに「Encryption Key」欄に半角英数字 8 文字以上の暗号コードを入力します。

7. 「Apply」にチェックが入っていることを確認し、「Submit」ボタンをクリックします。

SNMPv1 と SNMPv2 の設定情報にアクセスするためには、**LAN > Administration > SNMP Manager** を選択し、設定情報を含むページをクリックします。

1.4 サポートする機能

基本的なスイッチング機能に加え、D-Link 統合スイッチは以下の機能をサポートしています。

- 機能、環境にあわせた柔軟なオプション選択
- ギガポートを 24 ポート、SFP コンボポートを 4 ポート搭載
- 拡張ポート 2 ポート（DWS-3026）
- リダンダント電源サポート
- スイッチあたり 24 台（DWS-3026L）または 48 台（DWS-3026）の無線 AP を集中管理
- 4 台のスイッチをグループ化し 192 台の AP を集中管理
- アクセスポイントの自動検知
- 自動 RF チャンネル選択と AP Sentry モード
- 各種暗号、認証サーバに対応
- AP 認証、クライアント認証
- パワーマネージメント
- ロードバランス
- マルチ SSID
- 高速ローミング
- イントラスイッチローミング
- インターサブネットローミング
- リダンダント機能
- IP トンネリング
- L2+/L3 機能
- トラフィックモニタリング / 帯域制御
- SNMP v.1/v.2c/v.3、RMON
- IEEE 802.3af 給電機能
- GUI/CLI によるスイッチおよびアクセスポイントの設定 / 管理
- RoHS 指令対応

各アクセスポイントのサポート機能は、以下の通りです。

- IEEE 802.11b/g 準拠（DWL-3500AP）
- IEEE 802.11a（W52/W53）/b/g 準拠（DWL-8500AP）
- 108Mbps 無線通信（Turbo モード）
- デュアルバンド通信（DWL-8500AP）
- 5dBi ハイゲインデュアルアンテナ搭載
- 64/128/152 ビット WEP データ暗号化
- WPA/WPA2 エンタープライズで強力な暗号方式
- IEEE 802.1X ユーザ認証
- マルチ SSID（DWL-8500AP: 16 個、DWL-3500: 8 個）
- SNMP v.1/v.2c/v.3
- 侵入検知（不正 AP 検出、不正クライアント検出等）
- IEEE 802.1Q VLAN
- Telnet/SSH による設定
- IEEE 802.3af PoE 受電機能
- DWS-3024L/3026 による集中管理
- メタルシャーシ
- RoHS 指令対応

第 2 章　D-Link 統合アクセスシステム・ネットワークの設計

D-Link 統合アクセスシステムは、ご使用の無線デバイスとイーサネットデバイス間において、安定した高速なアクセスを提供します。本システムは、無線ネットワーク向けの、高機能かつ拡張性を兼ね備えた標準ベースのソリューションであり、最新の無線ネットワーク機能を実現するとともに WLAN（無線 LAN）の構築を可能にします。

本章は以下の項で構成されます。

- システム要件
- WLAN トポロジについて
- レイヤ 3 ローミング実現のためのネットワーク設計

2.1 システム要件

D-Link 統合スイッチ（統合スイッチ）の初期設定は設定用 PC と直接ケーブルを接続して行います。初期設定が行われると、統合スイッチの管理は Web ベースのユーザインタフェース（UI）、コマンドラインインタフェース（CLI）または SNMP で行うことができます。
以下に、D-Link 統合スイッチのインストールと管理をするために必要な条件を示します。

- VT100 端末、または端末エミュレーションソフトウェア搭載の PC
- D-Link 統合スイッチのコンソールポートとのシリアル接続
- Web ブラウザ、Telnet/SSH クライアントまたは SNMP マネージャ搭載の管理用リモートシステム

D-Link 統合アクセスシステムでセキュリティとネットワーク機能をサポートするためには、以下のオプションが必要となります。

- 無線クライアント、アクセスポイントおよびピア・無線スイッチの認証およびアカウント機能を提供する RADIUS サーバ
- VLAN をサポートしたネットワークデバイス
- スイッチおよびすべてのアクセスポイントにネットワーク情報を動的に割り当てる DHCP サーバ
- 外部ログ用 Syslog サーバ

図 2-1 は D-Link 統合アクセスシステムの設定と運用のための必要デバイスおよび任意のデバイスを組み込んだ基本的な構成を示しています。

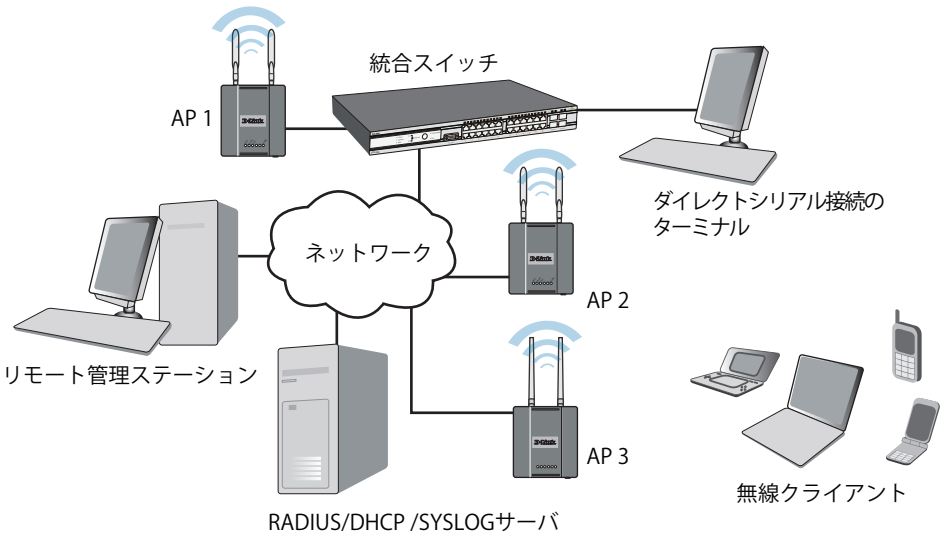


図 2-1　D-Link 統合アクセスシステム構成図

注意 D-Link 統合スイッチは DHCP サーバを内蔵しています。既存のネットワークに DHCP サーバが存在しない場合は、統合スイッチがネットワークホストにネットワーク情報を割り当てるよう設定をすることができます。

上の図で示すように、無線クライアントとは、ノートパソコン、PDA、スマートフォンなどの携帯型や据え置き型の Wi-Fi アダプタや無線サポートのドライバが装備されているデバイスを意味します。アクセスポイントに接続するためには、無線クライアントに以下に示すソフトウェアおよびハードウェアが搭載されている必要があります。

- アクセスポイントが準拠する 1 つ以上の IEEE 802.11 モードをサポートする、ポータブルまたは内蔵型の Wi-Fi クライアントアダプタ（IEEE 802.11a / 802.11b / 802.11g）
- WLAN と接続するよう設定したクライアントソフトウェア（例 : Microsoft Windows サプリカント）
- アクセスポイントで使用する認証モードに合致した、無線セキュリティソフトウェア

2.2 WLAN トポロジについて

D-Link 統合スイッチ（統合スイッチ）は、通常のレイヤ 2/3 スイッチが持つ基本的なスイッチングおよび IP ルーティング機能に、WLAN の機能が追加されています。ネットワークのどこに D-Link WLAN コントローラスイッチを導入するかについては、ネットワークの規模、要求事項、既存のトポロジによって異なります。既に存在するネットワークに無線ネットワークを拡張する場合と、十分な LAN のインフラストラクチャが無い環境に無線ネットワークを取り入れる場合では要求事項は違ってきます。

D-Link WLAN コントローラスイッチはレイヤ 2/3 スイッチング機能に加え WLAN データ転送と管理機能を持つため、D-Link アクセスポイント、PC やハブ、ルータ、スイッチなど他のネットワーク装置との間は、直接 統合スイッチの 10/100Mbps イーサネットポートで接続することができます。統合スイッチ自体は無線インタフェースをサポートしていないため、すべての接続は有線で行われます。

図 2-2 に示すように、D-Link WLAN コントローラスイッチは LAN スイッチでも WLAN スイッチでもあり、有線 LAN に接続するエンドユーザからのトラフィックも、アクセスポイントからのトラフィックも処理します。図 2-2 では、ビル 1 とビル 2 のそれぞれの各階に D-Link WLAN コントローラスイッチが設置されていることを示しています。

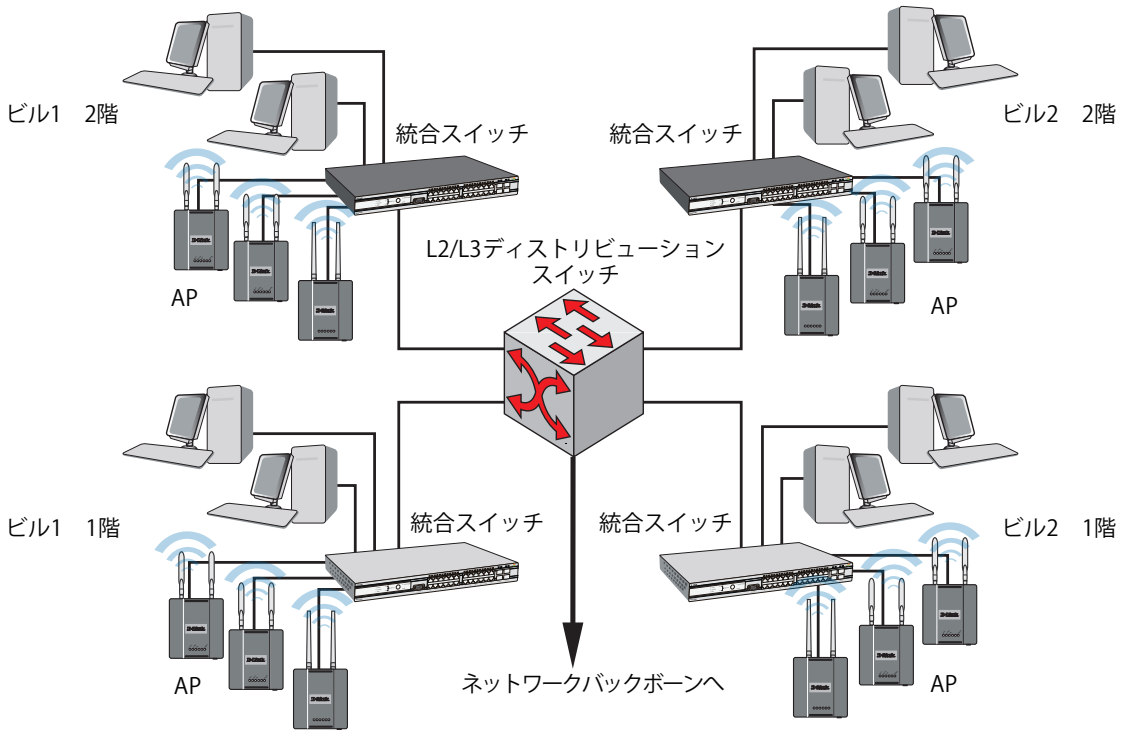


図 2-2　配線トポロジ

D-Link 統合スイッチは同じピアグループに属します。これにより無線クライアントはビルや各階を再認証の必要なしで移動することができます。さらにピア内の各統合スイッチは、それぞれの管理下にあるアクセスポイントと無線クライアントのリストを共有しているため、それらのアクセスポイントと無線クライアントは不正なもの（不明な存在）として見なされることはありません。

図 2-2 に示すようなトポロジは、ネットワーク上で LAN スイッチを追加、アップグレード、または交換する必要がある場合に便利です。

注意　トンネルクライアントがピアスイッチと共に使用される場合、ピアスイッチの一方は、トンネルクライアントのデフォルトゲートウェイとして設定される必要があります。通常、デフォルトゲートウェイはクライアントのサブネットから他のサブネットにすべてのトラフィックを送信しますが、ピアスイッチネットワークでは、クライアントが関連する AP を管理する統合スイッチは、リモートサブネットにフレームを送信します。つまり、各ピアスイッチはネットワーク内のあらゆるサブネットにフレームを送信することをルーティングテーブルエントリを持つ必要があるということを意味します。

図 2-3 はネットワークデータセンターに、2 台の D-Link WLAN コントローラスイッチ（統合スイッチ）を配置する構成です。この構成では、本スイッチはアクセスポイントやエンドユーザのノードに直接接続されていません。

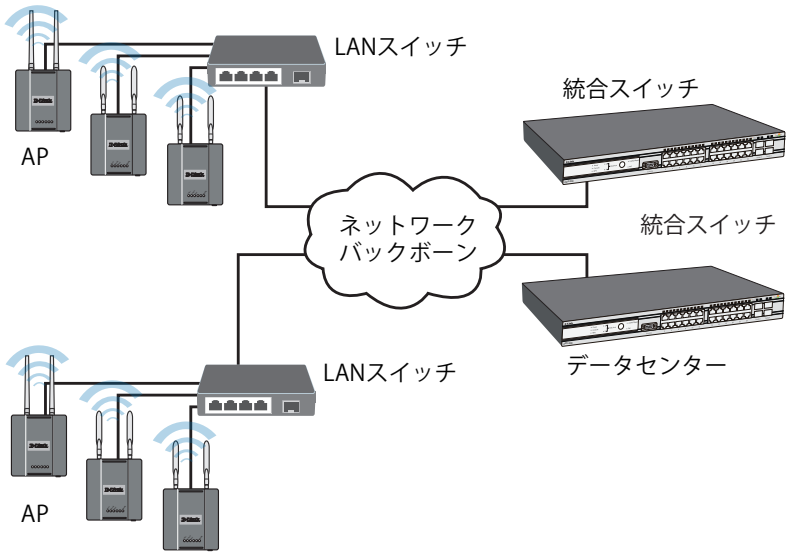


図 2-3　データセンタートポロジ

このようなデータセンタートポロジは既存のネットワークへの変更を最小限にしながら、無線 LAN ネットワークを追加したい場合に有効な方法です。無線クライアントからアクセスポイントへのトラフィックはトンネリングして統合スイッチを通過するか、またはアクセスポイントにより VLAN ID をタグ付けされて処理されます。タグ付けされたトラフィックは、統合スイッチを通過できない場合もあります。

アクセスポイント・スイッチ間の検出

アクセスポイントと統合スイッチがお互いを検出するためには、以下の 4 つの方法のいずれかを選択します。

- 統合スイッチの IP アドレスをアクセスポイントに登録する
- アクセスポイントの IP アドレスを統合スイッチに登録する
- DHCP オプション 43 を使用して DHCP サーバが統合スイッチの IP アドレスをアクセスポイントに配布するように設定する
- D-Link 無線デバイス・ディスカバリプロトコルを使用する

適切なアクセスポイントとスイッチ間の検出方法は、ご使用のネットワークトポロジによって異なります。例えば統合スイッチとアクセスポイントが同一のレイヤ 2 マルチキャストドメインに属する場合などは、D-Link 無線デバイス・ディスカバリプロトコルをご使用になることをお勧めします。

これらの選択肢についての詳細は、本マニュアル 36 ページの「4.5 アクセスポイントとピアスイッチの検出」を参照してください。

アクセスポイントの設置

D-Link アクセスポイントは、スイッチと同じサブネット、または異なるサブネットのどちらでも属することができます。アクセスポイントは、直接統合スイッチへ接続することも、他のネットワークデバイスへ接続することも可能です。D-Link アクセスポイントの無線伝送範囲は、約 100m ですが、環境条件の影響を受けて変化します。

最大限の無線伝送範囲を得るために、アクセスポイントの設置は以下のガイドラインに従って行ってください。

- 無線クライアントの動作位置を想定した場所に設置してください。
- 棚の上などの高い場所に設置すると、見通し距離を大きく確保できます。
- PC、電子レンジや 2.4GHz 帯使用のコードレス電話など、干渉の原因となるものの近くを避けて設置してください。
- 大きな金属面からなるべく遠ざけてください。
- 上下の範囲を広く確保する場合はアンテナを床に平行に設置し、逆に左右に広く確保するためには垂直に設置してください。
- アクセスポイントがそれぞれのブロードキャストの範囲内にある場合は、干渉を起こさない RF チャンネルを使用してください（802.11b/g の場合は 5 チャンネルの間隔を空ける）。

アクセスポイントの設置間隔は、RF 送信電力レベル、ネットワーク内の無線クライアントの数、またはアクセスポイントが使用するチャンネルによって異なります。RF 信号送信電力レベルはアクセスポイント信号のブロードキャスト範囲に直接影響を与えます。電力レベルが低すぎると、無線クライアントは信号検出ができなかったり、WLAN の品質低下につながります。逆に送信電力レベルが高すぎると、RF 信号は他のアクセスポイントと干渉を起こすこともあります。物理的にビルやネットワークの枠を超えた RF 信号のブロードキャストは、ネットワークにセキュリティ上の危険をもたらします。

送信電力レベルが高く RF ブロードキャストエリアが大きいほど、より多くの無線クライアントが信号を検出し、アクセスポイントと接続することができます。一般的には、アクセスポイントと接続する無線クライアントの数が多いほど、アクセスポイントが送受信するトラフィックも増大します。アクセスポイントでのネットワーク使用率を制限することにより、ネットワーク速度が遅くなることを防ぐことができます。しかし、アクセスポイントのネットワーク使用率が限界に達すると、新しく接続を試みるクライアントが接続拒否されることがあります。もし、ネットワーク使用率が頻繁に限界に達するようであれば、そのアクセスポイントの近くに、もう一台増設することをお勧めします。また、アクセスポイントが自動的にネットワーク環境に最適な送信電力とチャンネルの調整をするように設定をすることも可能です。

2.3 レイヤ 3 ローミング実現のためのネットワーク設計

D-Link 統合アクセスシステムでは、モバイルステーションはサブネットの異なるアクセスポイント間をローミング（行き来）しながら IP 接続を継続することができます。本機能は 802.11 のサブネット間で VoIP（Voice over IP）を実現するものです。

企業の IPv4 ネットワークは、いくつかのサブネットに分割する必要性がある場合があります。アクセスポイントは無線スイッチに直接接続されている場合や、スイッチからルータを使用していくつかのホップを経て接続されている場合もあります。

レイヤ 3 ローミングをサポートするためには、異なるサブネットを移動する際に無線クライアントの IP アドレスが変更されないように維持する必要があります。これは、無線クライアントがサブネットの境界を横切って移動する場合に IP 変換処理が行われないようにシームレスなローミングを保証します。

D-Link 統合アクセスシステムはローミングクライアントの IP アドレスの変更を防ぐ 2 つの方法を提供します。

1. VLAN と共にローミングするために SSID を関連させて、ご使用のネットワーク上のネットワーク装置が異なるサブネットをまたいで VLAN トランキングができるように設定可能です。これにより、クライアントは、移動中、同じ VLAN に所属し、同じ IP アドレスを保持することができるようになります。

   ネットワーク内のデバイスに VLAN トランキングを設定することが難しくない場合にこの手法は適しています。

2. トンネルされたサブネットでローミングするために SSID を関連つけることができます。この場合、本スイッチは、IP トンネリングを使用して管理下にあるアクセスポイントとの間にリンクを確立します。本スイッチはすべての IPv4 ユニキャストフレームのルーティングを行い、無線ネットワークはローカルで接続されているネットワークのように認識されます。

本スイッチ上では L3 ローミングをサポートするようにルーティングを有効にしておく必要があります。

図 2-4 は 1 台の無線クライアントが、異なるサブネットに属する 3 台のアクセスポイント間をローミングする様子を表しています。1 台の D-Link 統合スイッチ（統合スイッチ）は 3 台までのアクセスポイントの制御を行います。無線クライアントがいずれかのアクセスポイントと接続する時、L3 トンネルサブネットの統合スイッチから IP アドレスを受け取ります。クライアントがアクセスポイント間を移動する場合、WLAN との接続は保持され、スイッチが最初に割り当てた IP アドレスを使用し続けます。この時、クライアントが送受信するすべてのトラフィックはスイッチを通過します。

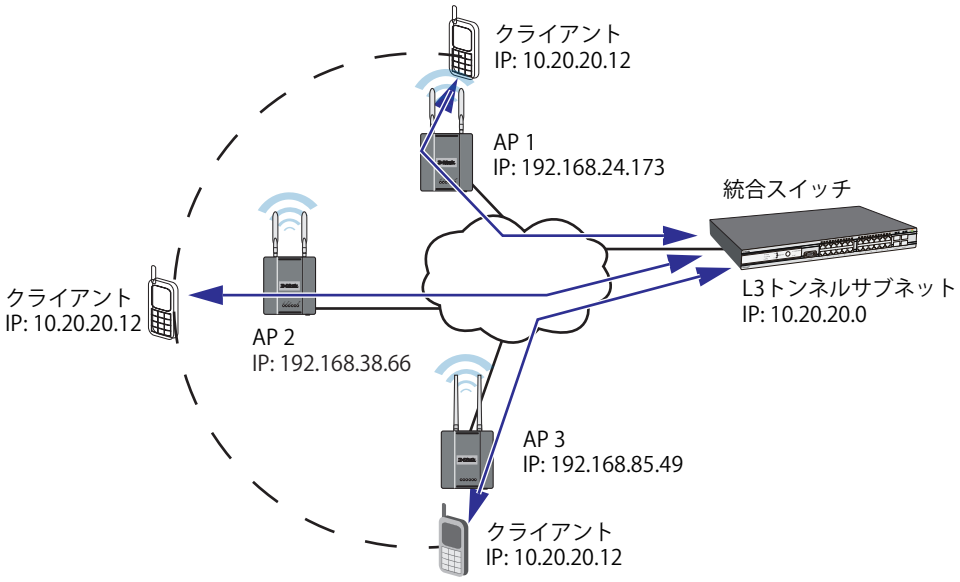


図 2-4　サブネット間ローミング

トンネリング設定では、ACL（アクセス制御リスト）や QoS パラメータを使用し、VoIP などのリアルタイム性の必要なトラフィックを他の WLAN トラフィックより優先させることができます。

IP 電話システムを使用する際は、ほとんどの場合、L3 トンネルサブネットの有線ポートとコールサーバを接続します。また、スイッチに DHCP リレーエージェントの設定をするか、またはスイッチが DHCP サーバの役割を果たすよう設定を行います。アクセスポイント、ピアスイッチ、および他のルータは L3 トンネルサブネットとの接続はできません。

L3 トンネリング機能についての詳細、またその設定方法については、65 ページの「L3 トンネル用 VAP の設定」および、146 ページの「付録 C L3 ローミング設定例」を参照してください。

第 3 章　ハードウェアの設置

本章では、D-Link の無線スイッチ DWS-3024L/3026 の設置について説明します。以下の手順に従って設置してください。

- ハードウェアの概要
  - 前面パネルの構成
  - LED 表示
  - 背面パネルの構成
  - 側面パネル
- 設置
  - パッケージ内容の確認
  - 設置前の準備
  - ゴム足の取り付け（19 インチラックに設置しない場合）
  - 19 インチラックへの取り付け
  - 電源をオンにする
  - SFP ポートへの取り付け
  - 拡張モジュールの取り付け
  - 外付けリダンダント電源システムへの接続
- スイッチの接続
  - スイッチとネットワークの接続
  - スイッチとアクセスポイントの直接接続
  - L2/L3 ネットワークを経由したスイッチとアクセスポイントの接続
  - 10GB アップリンクを使用したスイッチとコアネットワークの接続

3.1 ハードウェアの概要

本項では、スイッチの前面、背面、および側面パネルと、LED 表示について説明します。

前面パネルの構成

スイッチの前面パネルには、電源、コンソール、RPS（冗長電源システム）、PoE（Power over Ethernet）用 LED および各ポート用の Link/Act/Speed を示す LED、さらにオプションのモジュール実装時用の 10GE ポート（DWS-3026 のみ）と SPF ポート用の LED があります。

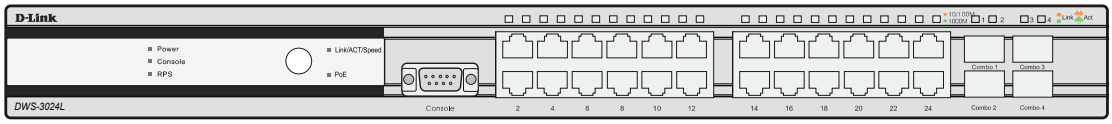


図 3-1　DWS-3024L の前面パネル図

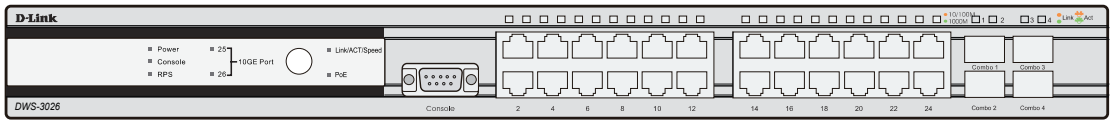


図 3-2　DWS-3026 の前面パネル図

LED 表示

スイッチは電源、コンソール、RPS、PoE 用 LED と、各ポートおよびオプションモジュール搭載時の 10GE ポート用 LED を装備しています。

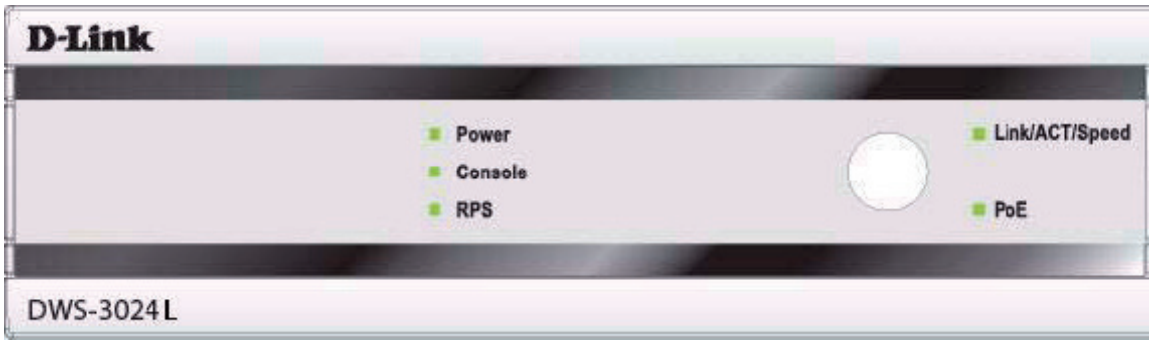


図 3-3　DWS-3024L の LED 表示

図 3-4　DWS-3026 の LED 表示

以下の表では、各スイッチの前面パネル上の LED およびモード選択ボタンについて説明します。

表 3-1　LED 仕様

LED 表示		色	ステータス	説明
Power		緑	点灯	電源が供給され正常に動作しています。
		ー	消灯	スイッチに電源が供給されていません（電源オフ時）。
Console		緑	点滅	電源投入後の Power ON Self Test(POST) 中点滅し、終了すると消灯します。
		緑	点灯	コンソールポートのリンクが確立しています。
RPS		緑	点灯	内蔵電源ユニットの異常により、拡張のリダンダント電源ユニットが動作しています。
		ー	消灯	リダンダント電源ユニットは動作していません。
Link/Act/Speed モード		緑	点灯	ポート LED でリンク、動作、速度を示します。Link/Act/Speed モードから PoE モードへ変更する時は、LED モード選択ボタンを押下します。
PoE モード		緑	点灯	ポートに接続されたデバイスによる 802.3af PoE（Power over Ethernet）電源供給状態を示すモードです。PoE モードから Link/Act/Speed モードへ変更する時は、LED モード選択ボタンを押下します。
ポート LED	前面パネルの 2 列のポートの上に 1 列のポート LED が配置されています。ポートの左上に位置する LED は、その直下の上段のポートの状態を示します。またポートの右上に位置する LED は、下段のポートの状態を示します。 ポート LED は、各ポートのリンク / 動作 / 速度を示す場合と、PoE の使用状態を示す場合があり、LED モード選択ボタンで切り替えます。			
	Link/Act/Speed モード	緑	点灯	ポートに 1000Mbps のリンクが確立されていることを示します。
		緑	点滅	ポート上でデータ転送中であることを示します（伝送速度 : 1000Mbps）。
		橙	点灯	ポートに 10Mbps または 100Mbps のリンクが確立されていることを示します。
		橙	点滅	ポート上でデータ転送中であることを示します（伝送速度 : 100Mbps）。
		ー	消灯	リンク / 動作のないことを示します。
	PoE モード	緑	点灯	給電中（802.3af 対応の受電デバイス検出）。
		橙	点滅	PoE ポートエラー。 IEEE 802.3af 非対応の受電デバイスの接続、IEEE 802.3af 低電流状態（電流 Imin 以下）、IEEE 802.3af 過電流状態（電流 I cut 以上）、ハードウェアエラーによりポート動作不能、供給可能電力超過、ショート検出、低電流・過電流の反復によるポートシャットダウン（受電デバイスの DC/DC エラーによるもの）等。
		ー	消灯	消灯時 - 給電なし（受電デバイスの検出なし、または接続なし）。
10GE ポート LED（DWS-3026 のみ）		緑	点灯	ポートにリンクが確立されていることを示します。
		緑	点滅	ポート上の動作（データ転送）を示します。
		ー	消灯	リンク / 動作のないことを示します。
Combo SFP LED		コンボポート用の LED はポート上部に位置し、Combo 1、Combo 2、Combo 3、Combo 4 と番号が振られています。		
		緑	点灯	リンクが確立しています。
		緑	点滅	ポート上の動作（データ転送）を示します。
		ー	消灯	リンク / 動作のないことを示します。

背面パネルの構成

電源コネクタは、標準の三極インレットです。ここに付属の電源ケーブルを接続し、電源プラグをコンセントに接続します。スイッチは供給電圧が100~240VAC、50~60Hz の間であれば自動的に電源設定を調整します。

背面パネルには、電源コネクタ、システムファン通気口、リダンダント電源コネクタ、さらにオプションの 10GE モジュール挿入用の 2 つの空きスロットがあります。電源に異常が発生した際には、オプションの外付けリダンダント電源システムがリダンダント電源コネクタに接続されていれば、瞬時かつ自動的にスイッチへの電源供給を開始します。

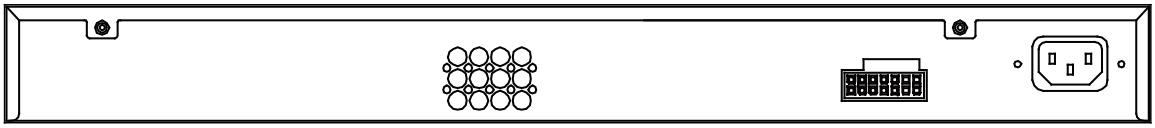


図 3-5　DWS-3024L 背面パネル図

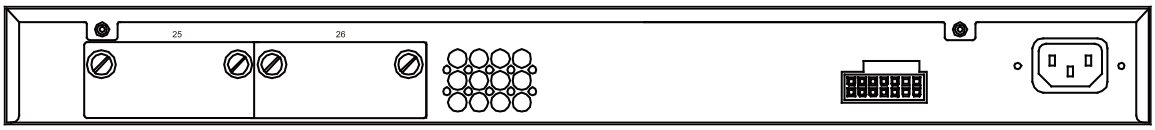


図 3-6　DWS-3026 背面パネル図

側面パネル

スイッチの両側に位置するシステムファンと排熱用通気口によって熱を放出するため、通気口を塞がないように注意してください。十分な通気のためには、装置の背面と側面には最低でも 15 センチ以上の空間を保つようにしてください。適切な熱放出、空気の循環をしないと、システム障害や部品の激しい損傷を引き起こす可能性があります。

3.2 設置

ここでは、スイッチを平らな場所や標準的な装置用ラックに設置する方法について説明します。また、オプションの設置についても説明します。

パッケージ内容の確認

ご購入いただいた製品の梱包箱を開け、内容物を注意して取り出してください。同梱物がすべてそろっているかをはじめにご確認ください。
万一、不足しているものがありましたら、弊社ホームページにてユーザ登録を行い、サポート窓口までご連絡ください。

☐ 本体 x 1 台
☐ 電源ケーブル x 1 本
☐ ラックマウントキット（ブラケット 2 枚、ネジ）
☐ ゴム足（裏面粘着）x 4 本
☐ RS-232C コンソールケーブル x 1 本
☐ CD-ROM（DWS-3000 シリーズ管理者用マニュアルと CLI MANUAL）x 1 枚
☐ 製品保証書

設置前の準備

スイッチの設置場所が性能に大きな影響を与えます。以下のガイドラインに従って本製品を設置してください。

- スイッチは、しっかりとした水平面で、最低 3 キロの耐荷重性のある場所に設置してください。スイッチの上に重いものを置かないでください。
- 電源コンセントはスイッチから 1.82m 以内としてください。
- 電源ケーブルが AC 電源ポートにしっかり差し込まれているか確認してください。
- スイッチから適切な熱分散が行われているか、またスイッチ周囲の通気が十分であるか確認してください。装置の前面と側面には最低でも 15 センチ以上の空間を保つようにしてください。
- スイッチは動作環境範囲内の温度と湿度に適応した涼しくて湿度の低い場所に設置してください。
- スイッチは強い電磁場が発生するような場所（モータの周囲など）や、振動、ほこり、および直射日光を避けて設置してください。
- スイッチを水平面に設置する際は、スイッチ底面に同梱のゴム足を取り付けてください。ゴム足はスイッチのクッションの役割を果たし、筐体自体や設置面に傷がつくのを防止します。

ゴム足の取り付け（19 インチラックに設置しない場合）

デスクトップや棚の上に設置する場合は、はじめに本スイッチに付属のゴム足をスイッチの裏面の四隅に取り付けます。スイッチの周囲に十分な通気を確保するようにしてください。

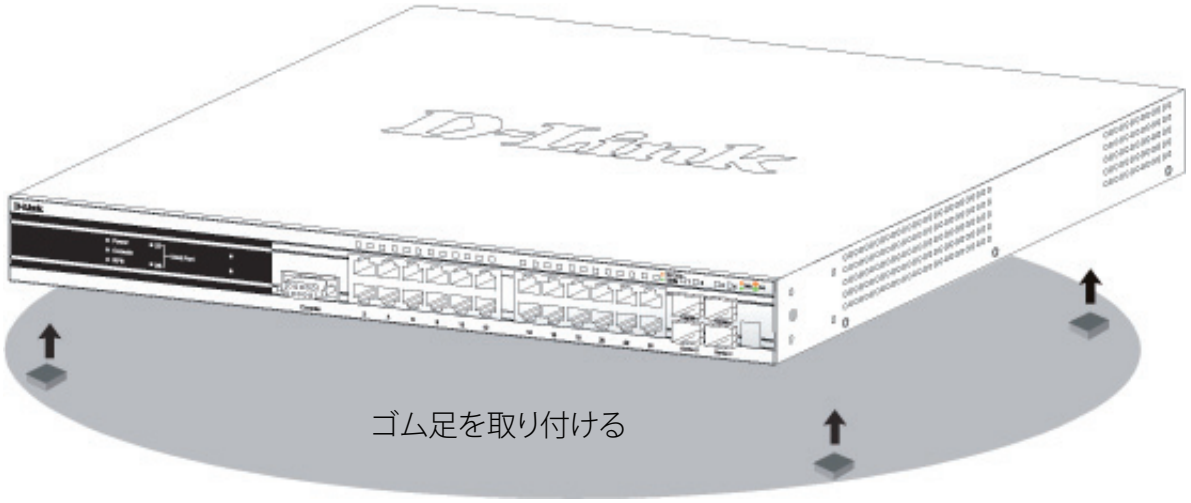


図 3-7　ゴム足の取り付け（デスクトップや棚の上に設置する場合）

19 インチラックへの取り付け

以下の手順に従って、本スイッチを標準の 19 インチラックに設置します。

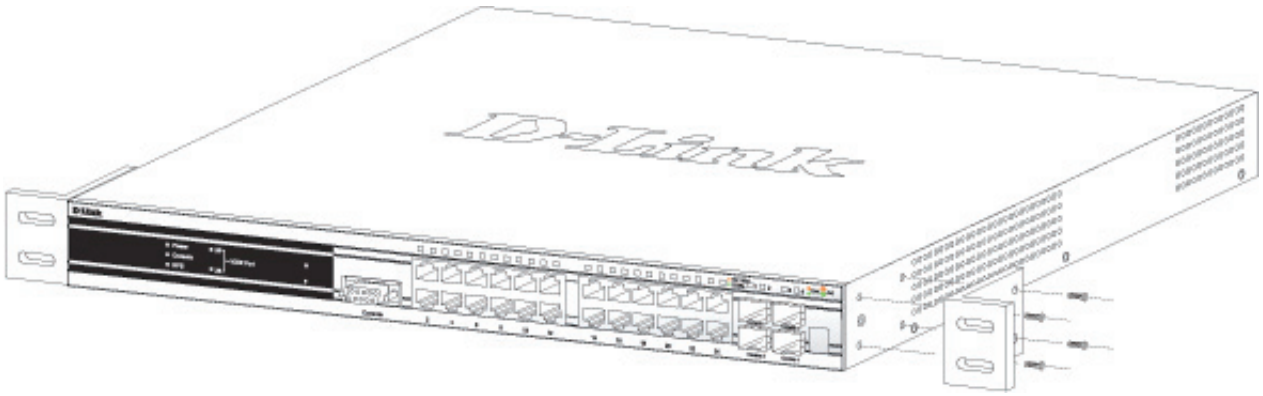


図 3-8　ブラケットを取り付ける

ラックマウントキットに付属のネジを使用して、本スイッチにブラケットを取り付けます。完全にブラケットが固定されたことを確認し、図 3-9 に示すように、本スイッチを 19 インチラックに固定します。

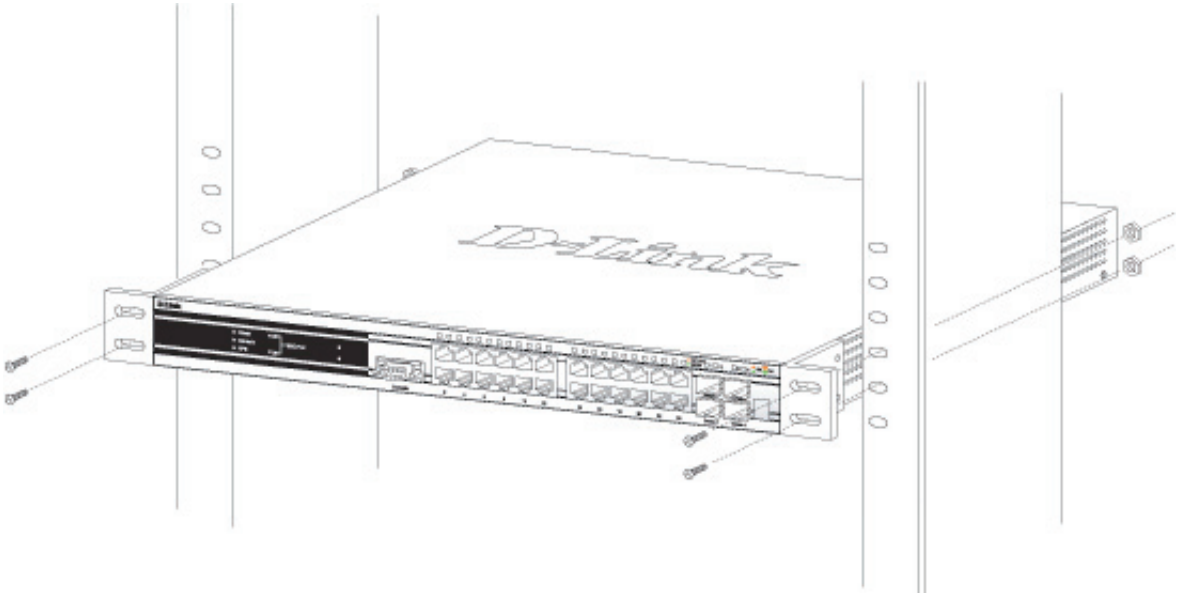


図 3-9　スイッチを 19 インチラックに設置する

電源をオンにする

電源ケーブルを本スイッチの電源コネクタに接続します。電源ケーブルのプラグを電源コンセントに接続します。

本スイッチに電源が供給されると、LED が点滅を始めます。この LED の点滅はシステムが再起動中であることを示しています。

SFP ポートへの取り付け

DWS-3000 シリーズスイッチは SFP（Small Form-Factor Pluggable）ポートを装備しています。本ポートは光ファイバトランシーバ用のケーブル配線に使用され、ギガビットデータ量の長距離伝送が可能なネットワークデバイスと通信を行います。これらのポートはフルデュプレックスとオートネゴシエーション機能をサポートし、D-Link 製の光トランシーバ DEM-310GT（1000BASE-LX）、DEM-311GT（1000BASE-SX）、DEM-314GT（1000BASE-LH）および DEM-315GT（1000BASE-ZX）と接続が可能です。SFP ポートの装着については以下の図を参考にしてください。

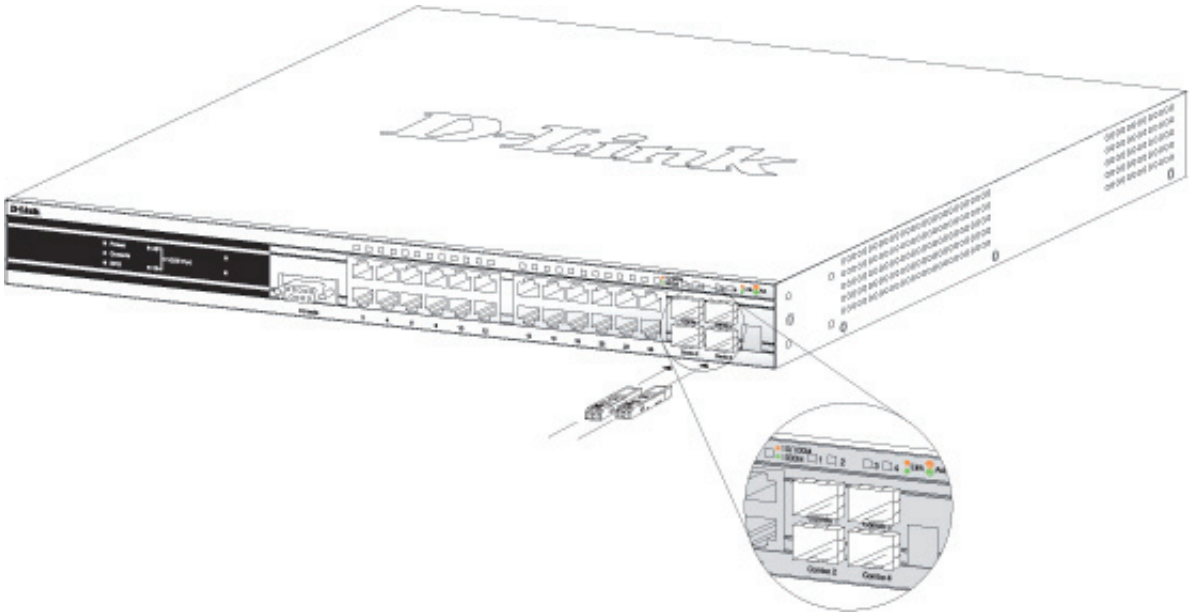


図 3-10　光トランシーバのスイッチへの装着

拡張モジュールの取り付け（DWS-3026 のみ）

背面パネルには、別売りの DEM-410X（1 ポート 10GE XFP アップリンクモジュール）、または DEM-410CX（ 1 ポート 10GBASE-CX4 アップリンクモジュール）を装着することのできる、2 つの空きスロットが用意されています。

警告　拡張モジュールの取り付けを行う前に、本スイッチからすべての電源ケーブルまたはケーブル類が取り外されていることを確認してください。取り外さないで作業を行うと、感電を引き起こし、人体やスイッチに損害を与えることがあります。

DEM-410X 拡張モジュールをスイッチに増設すると、10 ギガビット / 秒のデータ転送を可能にします。本モジュールポートは IEEE 802.3ae に準拠しており、フルデュプレックスのみをサポートし、XFP MSA に準拠したトランシーバのみ装着可能です。

DEM-410CX には光ファイバではなく銅線媒体を使用しています。本モジュールには CX4 コネクタを使用し、全二重モードでのデータ伝送を行います。

DWS-3026 スイッチにこれらのモジュールを装着する際は、本項に示す手順に従って行ってください。
これら拡張モジュールの装着用スロットはスイッチ背面に位置しています。これらのスロットを使用していない場合はスロットカバーを取り付けたままにしてください。モジュールの装着をする時は、スロットカバーのネジをゆるめて外してください。

拡張モジュールの前面パネルは、以下のような形状をしています。

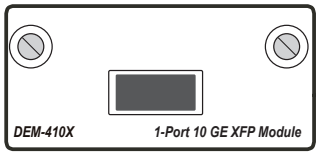


図 3-11　DEM-410X の前面パネル

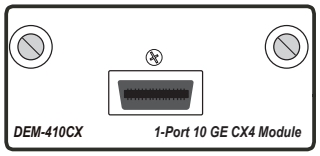


図 3-12　DEM-410CX の前面パネル

拡張モジュールの取り付け

空きスロットのスロットカバーを外す前には、電源ケーブルを抜いてください。モジュールを装着するには、以下の図のように、スイッチ背面の空きスロット内の奥に到達するまでモジュールをスライドさせます。注意しながらモジュールをゆっくり押し、ぴったりと固定します。

図 3-13　スイッチへの拡張モジュールの装着

次に、モジュール上の端の 2 本のネジを、スイッチ側のネジ穴に合わせて固定します。これでスイッチのアップグレードは完了です。

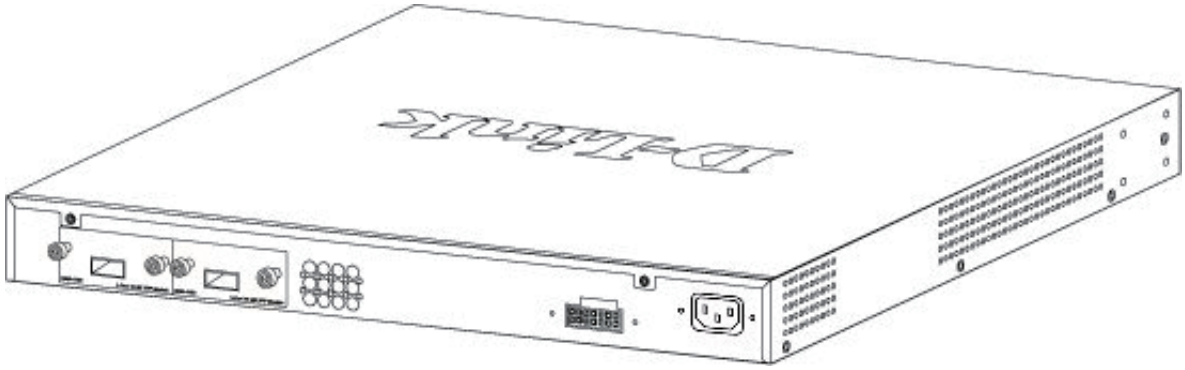


図 3-14　DEM-410X 拡張モジュール取り付け後のスイッチ

外付けリダンダント電源システムへの接続

本スイッチは外付けリダンダント電源システム（RPS）をサポートしています。以下の図は適切な RPS 電源とスイッチの接続状態を示しています。電源ケーブル、コネクタ、およびセットアップ手順については当該製品のマニュアルを参照してください。

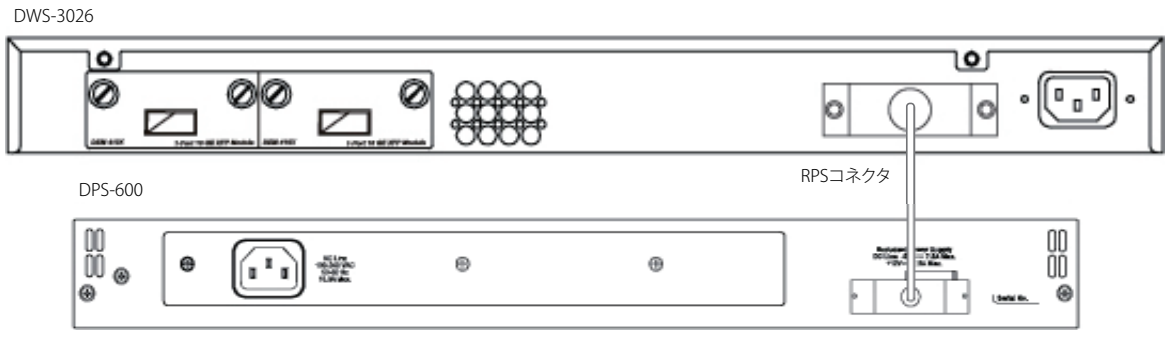


図 3-15　DPS-600 と本スイッチの接続

3.3 スイッチの接続

本項では以下のノード間の接続方法について説明します。

- スイッチとネットワークの接続
- スイッチとアクセスポイントの直接接続
- L2/L3 ネットワークを経由したスイッチとアクセスポイントの接続
- 10GB アップリンクを使用したスイッチとコアネットワークの接続

注意 すべてのイーサネットポートは Auto-MDI / MDI-X をサポートしています。

スイッチとネットワークの接続

本スイッチとネットワークの接続には 1000BASE-T ポート、10GB ポートまたは光ファイバポートが使用できます。どのタイプのポートを使用するかは、ネットワークの必要条件やスイッチと接続するノードの種類（ハブ、ルータ、他のスイッチ等）によって決定されます。

以下の接続方法があります。接続方法によって使用するケーブルは異なります。

- 本スイッチと 10BASE-T ハブまたはスイッチをカテゴリ 3、4、または 5 のツイストペア UTP/STP ケーブルを使用して接続する。
- 本スイッチと 100BASE-TX ハブまたはスイッチをカテゴリ 5 のツイストペア UTP/STP ケーブルを使用して接続する。
- 本スイッチと 1000BASE-T スイッチをエンハンスドカテゴリ 5 のツイストペア UTP/STP ケーブルを使用して接続する。
- 本スイッチの SFP ポートと光ファイバアップリンクサポートのスイッチを光ファイバケーブルで接続する。
- モード選択ボタンを使用して、本スイッチを PoE モードに変更する。PoE モード中、本スイッチは D-Link 802.3af 対応デバイスと接続できます。

各 UTP ポートの Link/Act LED は、有効なリンクが確立している時、緑または橙色に点灯します。同 LED が点滅している時は、そのポートでのデータの送受信が行われています。

スイッチとアクセスポイントの直接接続

DWL-3500AP や DWL-8500AP アクセスポイントと、ストレートまたはクロスの UTP ケーブルで直接接続することができます。

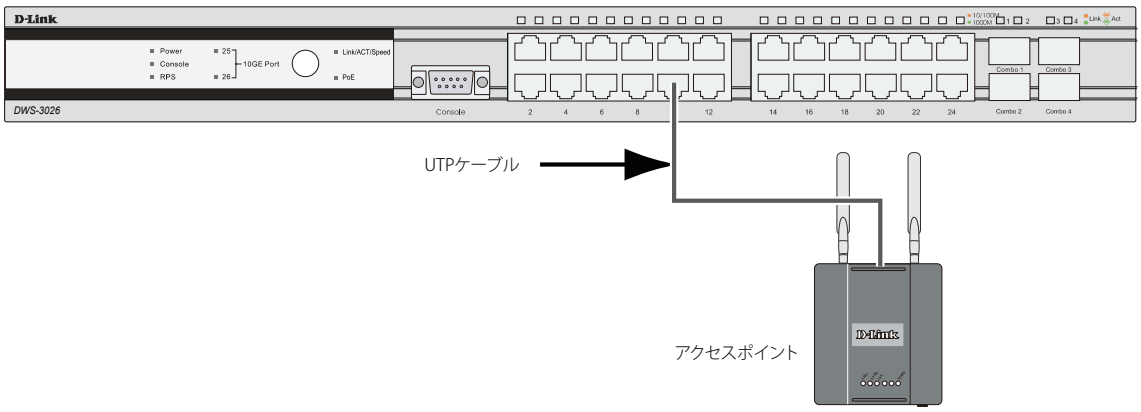


図 3-16　スイッチとアクセスポイントの直接接続

L2/L3 ネットワークを経由したスイッチとアクセスポイントの接続

本スイッチはアクセスポイントが直接接続されている場合、同一サブネット内のデバイス経由で接続されている場合、また他のサブネットに接続されている場合など接続方法にかかわらずアクセスポイントを検出して管理を行います。

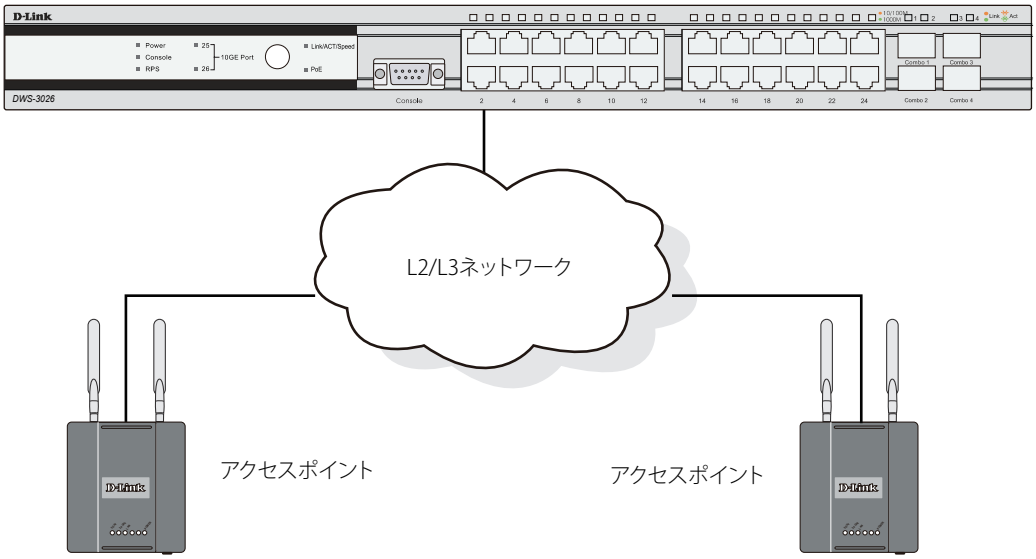


図 3-17　ネットワーク経由のスイッチとアクセスポイントの接続

10GB アップリンクを使用したスイッチとコアネットワークの接続（DWS-3026 のみ）

DWS-3026 のオプションの 10GB ポートはコアネットワークへのアップリンク接続に適しています。ギガビットイーサネットポートとの接続は、ポートの種類によって光ファイバケーブルまたはエンハンスドカテゴリ 5 ケーブルを使用します。正しくリンクが確立すると Link LED が点灯します。

図 3-18 では拡張モジュール DEM-410X を搭載した DWS-3026 の接続を示しています。

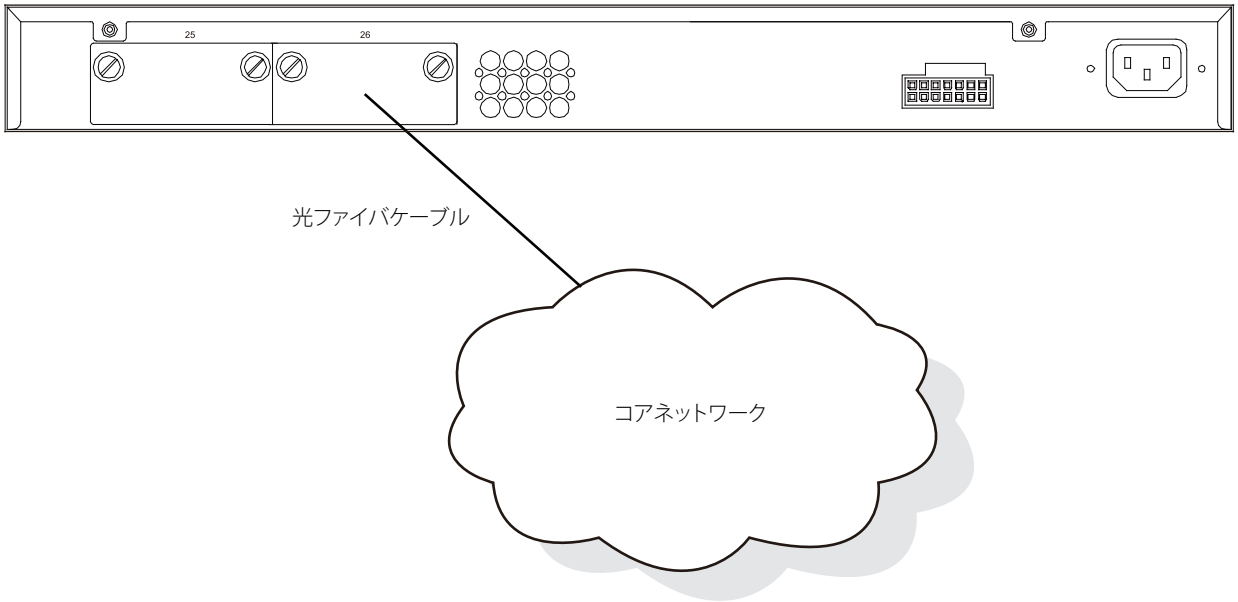


図 3-18　スイッチとコアネットワークの接続

第 4 章　D-Link 統合アクセスシステムの設定

本章では、以下の項の順に、統合アクセスシステムの設定をする方法について説明します。

- システムの設置について
- スイッチとネットワークの接続
- スイッチの WLAN 機能の有効化
- アクセスポイント側の準備
- アクセスポイントとピアスイッチの検出
- アクセスポイントの認証

4.1 システムの設置について

D-Link 統合アクセスシステムの設定および配置は、以下の標準的な手順に従って行います。

1. WLAN ネットワークトポロジを設計します。

無線クライアントから WLAN へのアクセスのしやすさを最大限にし、他のアクセスポイントからの電波干渉を最小にとどめるためには、どこにアクセスポイントを設置すべきか検討して決定します。また、D-Link 統合スイッチを既存のネットワークトポロジにどのように組み込むかについても検討します。WLAN トポロジの設計についての詳細な情報は、19 ページの「2.2 WLAN トポロジについて」を参考にしてください。

2. D-Link 統合スイッチのインストールと設定を行います。

スイッチのインストールと設定をするためには、スイッチに端末からシリアル接続をするか、スイッチのデフォルト IP アドレス（10.90.90.90/8）と同一サブネット内のホストから接続を行います。スイッチへの接続後、基本的なネットワークデータの設定やスイッチの DHCP クライアントの有効化を行うことができ、基本データを自動的に取得することが可能になります。

3. WLAN スイッチ機能を有効にし、WLAN スイッチインタフェースに IP アドレスを割り当てます。

WLAN スイッチ機能が有効場合にして、スイッチが D-Link アクセスポイントの検出および認証をすることができるようにします。ルーティングモードが無効の場合、統合スイッチはネットワークインタフェースの IP アドレスを使用します。ルーティング機能が有効の場合、スイッチは無線機能用にループバックインタフェースやルーティングインタフェースを使用します。
ネットワークインタフェースの IP アドレスを変更すると、自動的に無線機能が一旦無効になり、その後有効になります。ルーティング機能を有効にした場合も、無線機能は一旦無効になり、その後有効になります。初期値ではスイッチの WLAN 機能は有効です。

4. アクセスポイントがスイッチに認証された後に使用するデフォルト AP プロファイル設定を行います。

スイッチがアクセスポイントの認証に成功すると、スイッチからアクセスポイントに向けて AP プロファイルを送信します。AP プロファイルには電波帯域、セキュリティおよび SSID 設定などの、アクセスポイントの設定情報が含まれています。アクセスポイントの設定はスイッチからの認証の前でも後でもすることができます。デフォルト AP プロファイルの設定については、54 ページの「第 5 章 アクセスポイントの設定」を参照してください。

5. D-Link アクセスポイントの設置を行い、アクセスポイントからのスイッチ検出機能を有効にします。

アクセスポイントをネットワークに接続し、IP アドレスを取得（静的または DHCP を使用した動的割り付け）すると、無線スイッチは自動的にアクセスポイントを検出します。ただし、ご使用のネットワークが IEEE 802.1X 認証を使用しているか、スイッチからの検出時にアクセスポイントの認証を行いたい場合は、アクセスポイントにログインし、セキュリティ情報の設定を行う必要があります。

6. アクセスポイントと認証と確認を行います。

統合スイッチが認証したアクセスポイントのみを管理するように設定をすることもできます。アクセスポイントの認証にはローカルデータベース、または外部 RADIUS データベースが使用できます。アクセスポイントの認証が必要かどうかにかかわらず、スイッチはアクセスポイントの管理をする前に、アクセスポイントについて確認を行う必要があります。スイッチがアクセスポイントを確認するためには、各アクセスポイントの MAC アドレスをスイッチのデータベースか、または外部 RADIUS サーバのデータベースに登録する必要があります。

アクセスポイントの確認が成功すると、本スイッチでアクセスポイントの管理や、クライアントとの接続状況、使用状況、および統計情報を調べることができるようになります。本項の手順に従って設定すると、アクセスポイントはデフォルトコンフィグレーションプロファイルを取得します。デフォルトアクセスポイントプロファイルの設定内容については、138 ページの「付録 A」に掲載しています。

警告 デフォルトアクセスポイントプロファイルでは、無線クライアントの接続におけるセキュリティの設定をしていません。すべての無線クライアントがアクセスポイントや、ご使用のネットワークに接続可能な設定となっています。

無線クライアントからネットワークへの不正アクセスを防止するためには、アクセスポイントの配置をする前に、デフォルトプロファイルにセキュリティ設定をする方法と、Valid AP データベース（有効なアクセスポイントのデータベース）にアクセスポイントを登録する際、別のアクセスポイントプロファイルをそのアクセスポイントに割り当てる方法があります。デフォルトプロファイル設定に関する情報は、54 ページの「第 5 章 アクセスポイントの設定」を参照してください。

スイッチを使用して、ネットワークに配置するアクセスポイント向けに複数のアクセスポイントプロファイルを設定できます。各プロファイルには、RF 設定、QoS 設定、仮想アクセスポイント（VAP）設定などを定義します。アクセスポイントプロファイルの詳細については、54 ページの「5.1 アクセスポイントプロファイル、ネットワーク、ローカルデータベース」を、また新規アクセスポイントプロファイルの作成および登録方法については、108 ページの「8.1 アクセスポイントプロファイルの作成、設定、管理」を参照してください。

4.2 スイッチのネットワークへの接続

物理的なハードウェアの設置が完了したら、D-Link 統合スイッチをネットワークに接続します。スイッチのデフォルト IP アドレスは「10.90.90.90/8」で、DHCP は無効になっています。DHCP を有効にしたい場合や、違うスタティック IP アドレスを割り当てたい場合は、スイッチに接続して、初期設定を変更する必要があります。

スイッチへの接続は、Telnet 経由や、10.0.0.0/8 と同一のネットワークにあるホストの Web ブラウザを経由して行います。またはスイッチのコンソールポート（RS-232C DCE）を使用する方法もあります。スイッチと接続し、ネットワーク情報の設定や、DHCP クライアントの設定が可能です。

10.0.0.0 ネットワーク上のホストからスイッチに接続するためには、スイッチのデフォルト IP アドレス「10.90.90.90」を Web ブラウザか Telnet クライアントのアドレスフィールドに入力します。

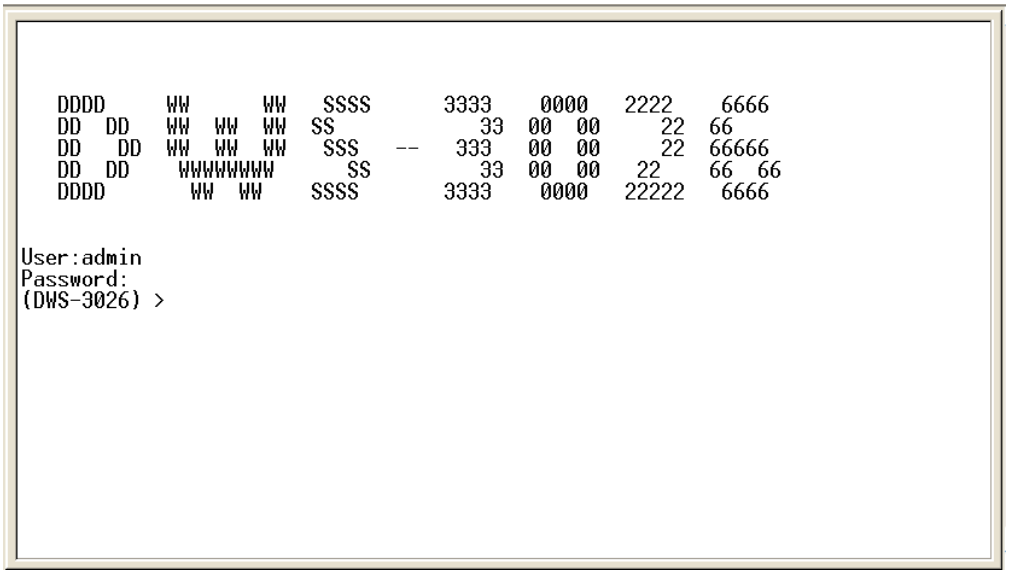
コンソールポートを使用したネットワーク情報の設定は、以下の手順で行います。

1. モデムケーブルを使用して、VT100/ANSI 端末かワークステーションをコンソール（シリアル）ポートに接続します。
   PC、Apple や UNIX のワークステーションと接続する場合は、ハイパーターミナルなどの端末エミュレーションプログラムを起動してください。

2. 端末エミュレーションプログラムの設定を以下に合わせてください。
   - データ速度 : 115,200bps
   - データビット : 8
   - パリティ : なし
   - ストップビット : 1
   - フロー制御 : なし

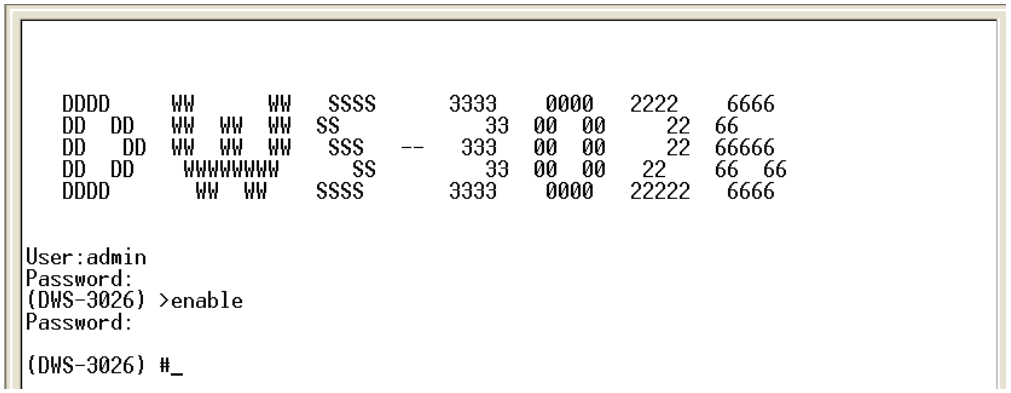
3. 「Enter」キーを押すと「User:」プロンプトが表示されます。
   ユーザ名に「**admin**」と入力してください。パスワードの初期設定はありません。パスワードの設定を行わない場合は、パスワードプロンプトが表示されたら「Enter」キーを押してください。

   ログインに成功すると、画面のプロンプトが （switch-prompt）> に変わります。



4. Privilege EXEC コマンドモードに遷移するために、(switch-prompt)> プロンプトの後に **enable** と入力します。Privilege EXEC コマンドモード用のパスワードの初期設定はありません。パスワードを変更しない場合は、パスワードプロンプトで「Enter」キーを押してください。

コマンドプロンプトは (switch-prompt)# に変わります。

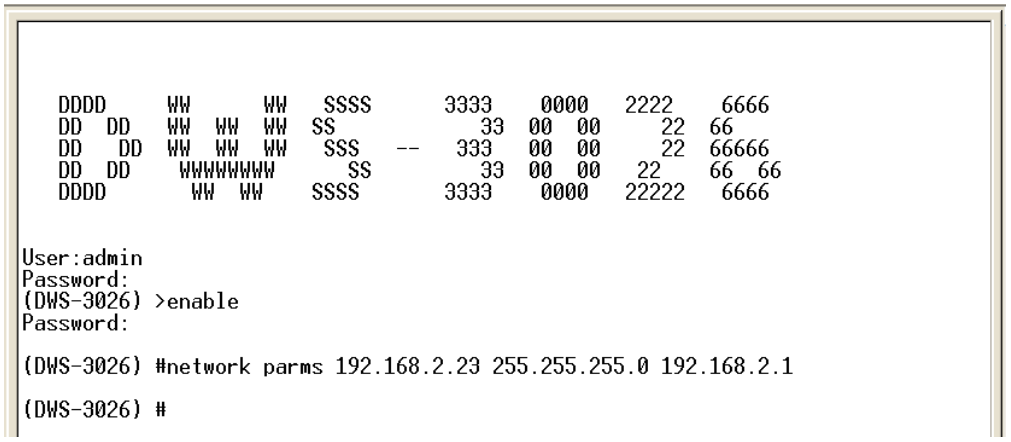


5. ネットワーク情報を登録します。

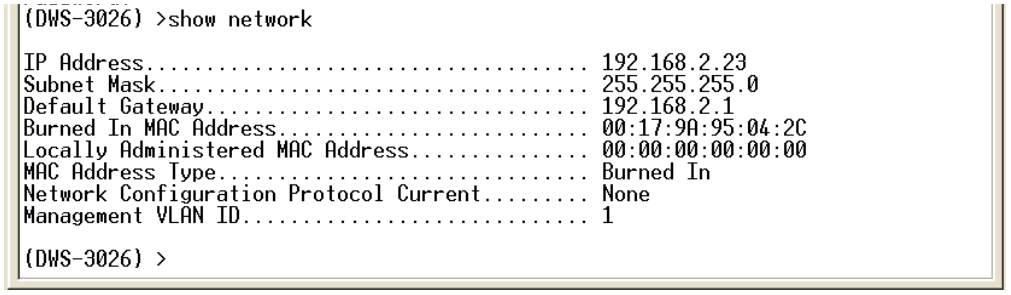
- DHCP サーバを使用して、IP アドレス、サブネットマスク、デフォルトゲートウェイ情報を取得するためには **network protocol dhcp** と入力します。
- BootP サーバを使用して、IP アドレス、サブネットマスク、デフォルトゲートウェイ情報を取得するためには **network protocol bootp** と入力します。
- IP アドレス、サブネットマスク、デフォルトゲートウェイ情報を手動で登録するためには、**network parms** <IP アドレス > < サブネットマスク > [< ゲートウェイ >] の順で入力します。

例 :**network parms 192.168.2.23 255.255.255.0 192.168.2.1**

デフォルトゲートウェイ情報は任意のパラメータなので、デフォルトゲートウェイ・アドレスは省略可能です。



ネットワーク情報を確認するためには **show network** と入力します。



6. これらの設定を保存し、スイッチのリセット時も保持されるようにするためには、以下のコマンドを入力します。

```
write memory
```

一度 D-Link WLAN コントローラがネットワークに接続すると、割り当てられた IP アドレスを使用して、Web ブラウザ、または Telnet、SSH を経由してスイッチにリモートアクセスが可能になります。

4.3 スイッチの WLAN 機能の有効化

統合スイッチがアクセスポイントの検出と管理を行うためには、WLAN スイッチ機能とその操作ステータスをともに有効にする必要があります。WLAN コンポーネントは初期値で有効です。スイッチのユーザインタフェースに接続する場合、スイッチに正しい国コードが設定されていることを確認します。アクセスポイントが本製品を日本で許可されるモードで動作できるように、WLAN スイッチ機能を有効にする前に、まず国コードを「JP」（日本）に変更します。国コードの初期値は「US」（アメリカ合衆国）となっています。

Web インタフェースを使用して、国コードを「JP」に変更します。

WLAN > Administration > Basic Setup の順にメニューをクリックし、「Global」タブの「Wireless Global Configuration」画面を表示します。表 4-1 に各項目について説明します。

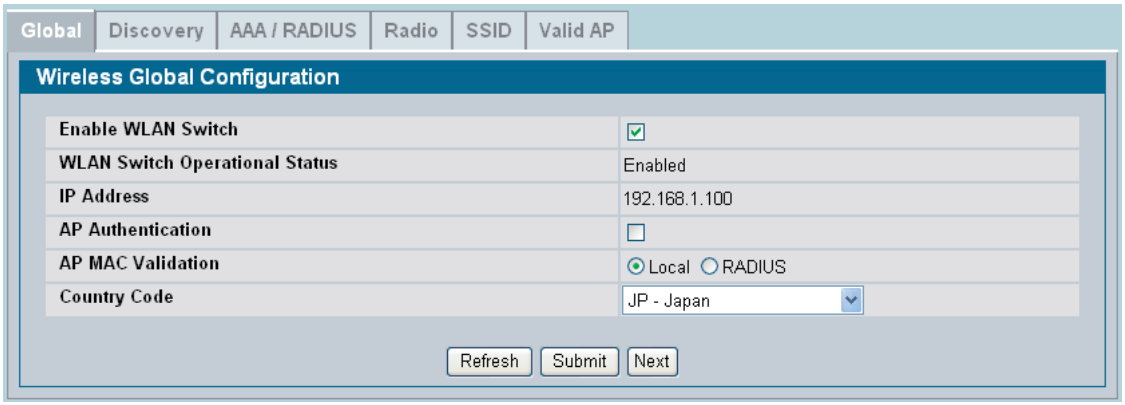


図 4-1　Wireless Global Configuration 画面

注意　無線機能に関する設定はナビゲーションメニュー中の「WLAN」タブで行います。

注意　多くの設定ページには「Submit」ボタンがあり、そのボタンをクリックすることで現在の設定に変更を加えることができます。しかし、その変更は不揮発性メモリ（NVRAM）には保存されません。再起動後も変更を有効にする場合は、「Tool」メニューの「Save Changes」をクリックし、適切なページへ移行してください。または、CLI の Privilege EXEC モードで **`write`** コマンドを実行する方法もあります。

表 4-1　無線グローバル基本設定（Global タブ）

設定項目	説明
Enable WLAN Switch	ボックスにチェックを入れると、システムの WLAN スイッチ機能を有効にします。WLAN スイッチ機能を無効にするためには、チェックを外してください。 チェックを外すと、本スイッチに接続中のピアスイッチやアクセスポイントは切断されます。 WLAN スイッチ機能を無効にしても、VLAN や STP などのその他の機能には影響しません。
WLAN Switch Operational Status	スイッチの稼動状況を表示します。以下のいずれかが表示されます。 • Enabled - 有効。 • Enable-Pending - 有効保留中。 • Disabled - 無効。 • Disable-Pending - 無効保留中。 状況が保留中の場合は「Refresh」をクリックして画面を更新してください。
WLAN Switch Disable Reason	WLAN スイッチ機能が無効である場合、本項目が現れて以下の原因の一つが表示されます。 • None - WLAN スイッチ機能無効の原因が不明です。 • Administrator disabled -「Enable WLAN Switch」チェックボックスのチェックが外されました。 • No IP Address - WLAN インタフェースに IP アドレスが割り当てられていません。 • No SSL Files - D-Link 統合スイッチは、アクセスポイントと SSL 暗号化通信を行っています。統合スイッチの電源を投入すると、自動的にサーバ証明書が発行され、SSL 接続の確立に使用されます。SSL 証明書およびキーの発行には約 1 時間を要します。 スイッチ上でルーティングが有効になっていても、稼動状況は以下の原因で無効とされている場合があります。 • No Loopback Interface - スイッチにループバックインタフェースが存在しません。 • Global Routing Disabled - グローバルルーティングが無効です。稼動状況を有効にするためには、WLAN スイッチインタフェース上でルーティングモードだけでなく、グローバルルーティングも有効にする必要があります。 ループバックインタフェースの設定と、ルーティングを有効にするための情報については、39 ページの「ルーティング機能を有効にした D-Link 統合スイッチ」を参考にしてください。
IP Address	スイッチの WLAN インタフェースの IP アドレスが表示されます。ルーティング機能を無効にしている場合、表示される IP アドレスはネットワークインタフェースです。ルーティング機能を有効にしている場合は、統合スイッチ機能用に登録したルーティングインタフェースまたはループバックインタフェースが表示されます。
AP Authentication	アクセスポイントがスイッチと接続する際に認証が必要な場合は、ボックスにチェックを入れます。

設定項目	説明
AP MAC Validation	アクセスポイントの認証に使用するデータベースを選択します。 • Local - ローカル Valid AP データベースに各アクセスポイントの MAC アドレスを登録する必要があります。 • RADIUS - 外部 RADIUS サーバに各アクセスポイントの MAC アドレスを登録する必要があります。
Country Code	国コード。国コードを「JP」に変更します。変更する際には、変更を確認するポップアップ画面が表示されます。 無線通信に関する規則は国ごとに異なります。正しい国コードを選択し、WLAN システムが運用する国の規則を遵守するようにしてください。国によっては、Atheros モードなどの様に使用できない WLAN モードがあります。 国コードの変更により、スイッチは有効または無効に切り替えられます。チャンネルおよび、無線モードの設定のうち、その地域の規則に対して妥当でないものは、初期値にリセットされます。 国コードは beacon フレームや prove Response に乗せてアクセスポイントから送信されます。

CLI で、管理者モード（Privilege EXEC モード）で「**show wireless**」コマンドを実行して、同様の情報を確認することができます。国コードの変更を行う必要がある時は、「**show wireless country-code**」コマンドを実行して、選択可能な国名と 2 文字のコードリストを確認できます。

国コードの設定と、WLAN スイッチ機能を有効にするコマンドは、「Wireless Config」モードで実行できます。国コードを設定するためには、「**country-code** <code>」と入力してください。WLAN スイッチ機能を有効にするためには、「**enable**」と入力します。以下に、「Wireless Config」モードへ遷移して、国コードを日本に設定し、WLAN スイッチ機能を有効にするためのコマンド実行例を示します。

```
(switch-prompt) #configure
(switch-prompt) (Config)#wireless
(switch-prompt) (Config-wireless)#country-code jp
(switch-prompt) (Config-wireless)#enable
```

4.4 アクセスポイント側の準備

ネットワークのセキュリティのため、ネットワーク接続前に、アクセスポイントの CLI に接続していくつかの設定が必要です。初期値では、アクセスポイントはタグなしの VLAN を使用し、セキュリティ設定は行われていません。IEEE 802.1X 認証が必要である場合は、ネットワークに接続する前に、アクセスポイントのサプリカント情報の設定をする必要があります。また、D-Link 統合スイッチがローカル AP 認証を要求する設定を行う場合は、アクセスポイントの CLI に接続してパスフレーズを登録します。無線クライアントから AP の管理用インタフェースへの接続を防ぐためには、管理用 VLAN を構築する方法があります。

注意 アクセスポイントでコマンドを実行すると、現在の設定に変更を加えることができますが、その変更は不揮発性メモリ（NVRAM）には保存されません。再起動後も変更を有効にする場合は「**save-running**」コマンドを実行してください。

アクセスポイントへのログイン

アクセスポイントの CLI には Telnet によるアクセスのみが可能です。IP アドレスの初期値は 10.90.90.91/8 で、DHCP クライアントの初期設定は有効です。アクセスポイントは、DHCP サーバの存在するネットワークに接続されると自動的に IP アドレスを取得します。ネットワーク上に DHCP サーバが存在しない場合は、アクセスポイントは、スタティック IP アドレスが登録されるまで IP アドレスの初期値 10.90.90.91/8 を保持します。

初期設定を直接イーサネットで接続して行う場合は、使用する PC が 10.0.0.0/8 サブネット内の IP アドレスを持つことを確認してください。

UTP ケーブルで直接接続する場合は、以下のように、UTP ケーブルでアクセスポイントの LAN ポートと PC の LAN ポートに接続します。

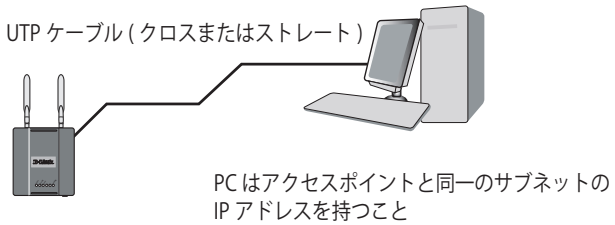


図 4-2　スタティック IP 登録のためのイーサネット接続

この方法で設定を行った後、アクセスポイントの起動および実際の運用をするためには、設定用 PC との接続を切り離してネットワークと接続します。

アクセスポイントの CLI に Telnet により接続すると、「DLINK-WLAN-AP login:」というプロンプトが表示されます。
ユーザ名に「**admin**」と入力し、パスワードにも「**admin**」と入力します。ログインに成功するとプロンプトは「DLINK-WLAN-AP#」に変わります。

DHCP クライアント機能を無効にしたり、スタティック IP アドレスの登録する方法については、39 ページの「スイッチと管理対象のアクセスポイントへの IP アドレスの割り当て」の 41 ページの「D-Link アクセスポイント」を参照してください。

アクセスポイントパスワードの変更

アクセスポイントに接続するためには、ユーザ名（admin）とパスワード（admin）の入力が必要です。セキュリティを高めるために、パスワードの初期値を変更することをお勧めします。

デフォルトパスワードを変更するためには、アクセスポイントにログインし、以下のコマンドを実行します。

```
set system password < パスワード >
```

例として、パスワードを test1234 に変更するコマンドを示します。

```
set system password test1234
```

入力したパスワードはテキスト表示されます。一度入力した後に、確認を求められることはありません。

注意 パスワードは忘れないように書き留めておいてください。パスワードには半角英数字 8 ～ 63 文字を入力します。

アクセスポイントでの 802.1X 認証情報の設定

IEEE 802.1X のポートベースのネットワークアクセス制御を利用するネットワークでは、サプリカント（クライアント）は 802.11x オーセンティケータにアクセスが許可されるまで、ネットワークへアクセスすることができません。ネットワークで 802.1X 認証が使用されている場合は、アクセスポイントに 802.11x 認証情報を登録する必要があります。

注意 アクセスポイントは MD5 認証をサポートしています。

表 4-2 に 802.1X のサプリカント情報を登録するためのコマンドを示します。

表 4-2　IEEE 802.1X サプリカントコマンド

アクション	コマンド
802.1X サプリカントについての設定を表示する	**get dot1x-supplicant**
802.1X サプリカント機能を有効にする	**set dot1x-supplicant status up**
802.1X サプリカント機能を無効にする	**set dot1x-supplicant status down**
802.1X ユーザ名を登録する	**set dot1x-supplicant user <** ユーザ名 **>**
802.1X パスワードを登録する	**set dot1x-supplicant password <** パスワード **>**

以下の例では、管理者が 802.1X サプリカント機能を有効にし、ユーザ名を wlanAP、パスワードを test1234 と登録しています。

```
WLAN-AP#set dot1x-supplicant status up
WLAN-AP#set dot1x-supplicant user wlanAP
WLAN-AP#set dot1x-supplicant password test1234
WLAN-AP#get dot1x-supplicant
Property Value
--------------------------
status   up
user     wlanAP
```

アクセスポイントからスイッチ側への認証情報の設定

アクセスポイントにパスフレーズを登録し、認証されたアクセスポイントのみがスイッチと接続できるようにします。統合スイッチ側でアクセスポイントの認証を有効にした場合、アクセスポイント側の CLI に接続し、パスフレーズを登録する必要があります。このパスフレーズは統合スイッチ側で登録したものと同じに設定します。

アクセスポイントにパスフレーズを設定するためには、以下のコマンドを実行してください。

```
set managed-ap pass-phrase < パスフレーズ >
```

パスフレーズは半角英数字 8 ～ 63 文字（大文字、小文字の区別あり）で設定します。

以下のコマンド例では、アクセスポイントから統合スイッチへの認証パスフレーズを test1234 と登録しています。

```
WLAN-AP#set managed-ap pass-phrase test1234
```

アクセスポイントと統合スイッチ間の認証についての詳細情報と、統合スイッチ上での設定方法については、48 ページの「アクセスポイント認証の設定」を参照してください。

アクセスポイントでの VLAN 情報設定

管理用 VLAN はデフォルトで VLAN 1 に指定されています。本 VLAN は初期値でタグなし VLAN です。つまり、この VLAN では、管理用トラフィックを含むすべてのトラフィックがタグなしです。

アクセスポイントの管理インタフェースへのアクセスを制限したい場合や、ネットワーク上に異なる VLAN ID を使用した管理用 VLAN が存在している場合は、アクセスポイントの管理用 VLAN の VLAN ID を、アクセスポイントの CLI を使用して、変更することができます。

表 4-3　AP VLAN コマンド

アクション	コマンド
VLAN ID を含む管理インタフェース情報を表示する	**get management**
管理用 VLAN ID を登録する	**set management vlan-id** <1-4096>
タグなし VLAN 情報を表示する	**get untagged-vlan**
タグなし VLAN を有効にする	**set untagged-vlan status up**
タグなし VLAN を無効にする	**set untagged-vlan status down**
タグなし VLAN ID を登録する	**set untagged-vlan vlan-id** <1-4096>

4.5 アクセスポイントとピアスイッチの検出

D-Link 統合スイッチは以下のデバイスの検出、確認、認証および監視を行います。

- ピア無線スイッチ
- D-Link アクセスポイント
- 無線クライアント
- 不正アクセスポイント
- 不正無線クライアント

ここでは、D-Link アクセスポイントや他の D-Link 統合スイッチを検出する手順を説明します。無線クライアントの検出については、99 ページの「7.7 接続中のクライアントのモニタ」を、また不正なデバイスの検出については、97 ページの「7.6 不正アクセスポイントのモニタとアクセスポイントの RF スキャン」を参照してください。

統合スイッチが他の WLAN デバイスを検出し通信を確立するためには、それらのデバイスに IP アドレスが設定され、他の WLAN デバイスの検出が可能で、かつ統合スイッチと互換性を持つ必要があります。

D-Link 統合スイッチが、D-Link アクセスポイントを検出し認証する時、スイッチはそのアクセスポイントの管理も開始します。初期状態のアクセスポイントプロファイル設定内容は、138 ページの「付録 A」を参照してください。

アクセスポイントプロファイル設定の変更方法は 54 ページの「第 5 章 アクセスポイントの設定」を参照してください。

検出方法

統合スイッチとアクセスポイントがお互いの検出をするためには、いくつかの方法があります。以下に検出方法の例を説明します。

例 1 : レイヤ 2 検出

図 4-3 では、アクセスポイントと統合スイッチは直接接続されています。どちらのデバイスも同じレイヤ 2 のブロードキャストドメインに属し、デフォルト VLAN 設定を使用しています。

双方のデバイスが、静的にまたは DHCP を使用して IP アドレスを取得すると、統合スイッチは自動的に L2 Discovery メッセージをブロードキャストしてアクセスポイントを検出します。

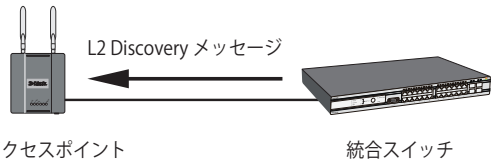


図 4-3　レイヤ 2 でのデバイス検出例

この例では、管理者はアクセスポイントや統合スイッチに対して検出情報の設定を行う必要はありません。レイヤ 2 でのデバイス検出は、デバイスが直接接続された時、またはレイヤ 2 ブリッジを使用して接続された時に自動的に実行されます。

デバイス検出方法についての詳細情報は、42 ページの「D-Link 無線デバイス検出プロトコル」を参照してください。

例 2 : アクセスポイントの IP アドレスをスイッチに登録

図 4-3 には 2 台のアクセスポイントがあります。1 台は D-Link 統合スイッチと直接接続され、もう一台は L3 スイッチを経由して接続されています。

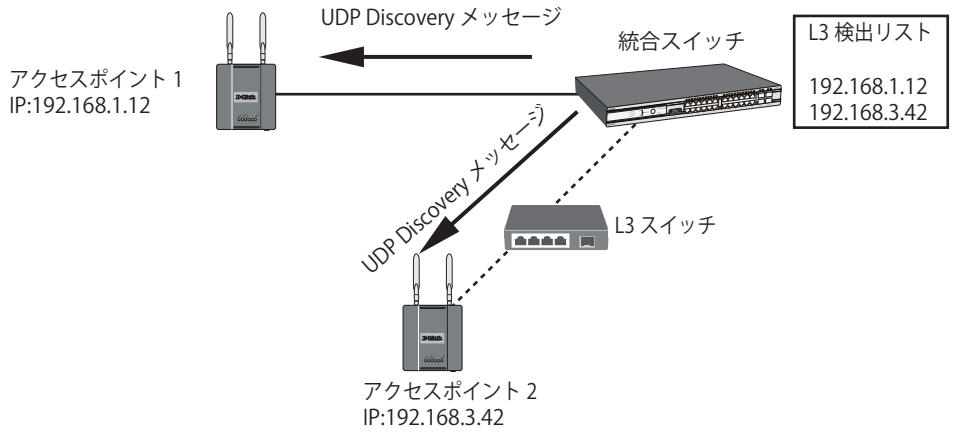


図 4-4　レイヤ 3 でのデバイス検出例 1

管理者は、スイッチ上でレイヤ 2 検出メソッドを無効にし、両方のアクセスポイントの IP アドレスを L3 検出リストに登録します。統合スイッチはリスト中の IP アドレスに対して、UDP Discovery メッセージを送信します。アクセスポイントがそのメッセージを受信し、そのスイッチに接続できることを確認すると、スイッチに対し SSL による TCP 接続を開始します。

本検出方法についての詳細は 43 ページの「スイッチにピアスイッチとアクセスポイントの IP アドレスを登録する」を参照してください。

例 3 : スイッチの IP アドレスをアクセスポイントに登録

この例では、管理者はアクセスポイントの CLI に接続し、アクセスポイントを管理する 2 台の D-Link 統合スイッチの IP アドレスを静的に登録します。

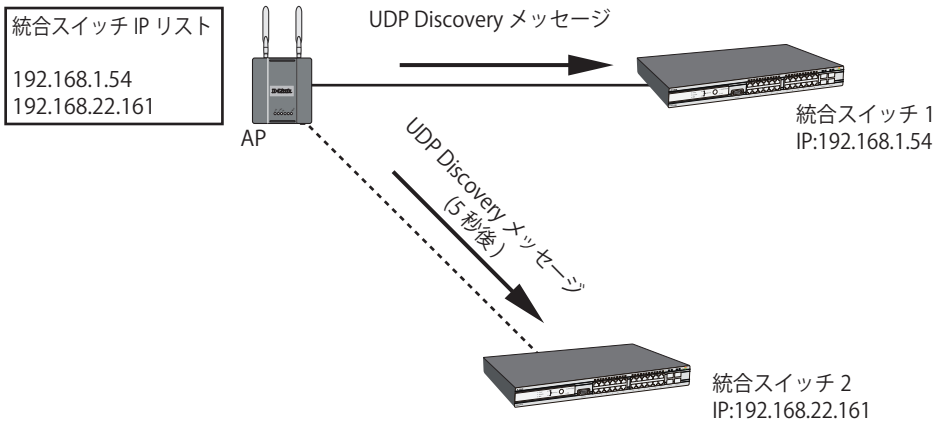


図 4-5　レイヤ 3 でのデバイス検出例 2

アクセスポイントは、UDP Discovery メッセージをリスト中の一番目の IP アドレス宛てに送信します。統合スイッチがそのメッセージを受信すると、そのアクセスポイントの Vendor ID は有効であるか、アクセスポイントに SSL による TCP 接続が既に存在していないか、また管理するアクセスポイントの最大数に達していないかを確認します。すべての条件が整ったら、統合スイッチはアクセスポイントに対し invitation メッセージを送信し、SSL による TCP 接続を開始します。

リスト中 1 番目の統合スイッチから invitation メッセージを受信しないと、最初の統合スイッチへの UDP Discovery メッセージ送信から 5 秒後に、2 番目の統合スイッチに向けて UDP Discovery メッセージを送信します。

アクセスポイントに統合スイッチの IP アドレスの登録がされていれば、他のスイッチが別の方法でアクセスポイントを検出しても、そのアクセスポイントは登録済みスイッチとだけ接続をします。

このようなデバイス検出方法についての詳しい情報は、45 ページの「D-Link アクセスポイントにスイッチの IP アドレスを登録する」を参照してください。

例 4 : DHCP オプション

この例では、管理者はアクセスポイントから DHCP サーバに送信する DHCP Request に対してリプライされる DHCP Response 中のオプションとして統合スイッチの IP アドレスを設定します。

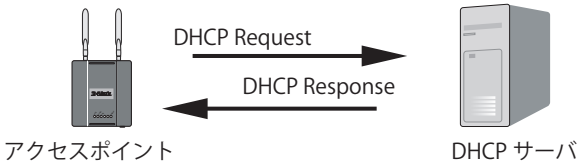


図 4-6　DHCP オプションを使用する例

アクセスポイントは DHCP Response 中の DHCP オプション 43 に、最大 4 台までの統合スイッチの IP アドレスまたは DNS 名を設定できます。

この検出方法は、アクセスポイントが DHCP サーバからネットワーク情報を受信する前に、DHCP オプションの設定が行われている場合のみ有効となります。

DHCP オプション 43 に統合スイッチの IP アドレスを設定する方法については、46 ページの「DHCP オプションにスイッチ情報を設定する」を参照してください。

検出とピアスイッチ

ネットワーク中に複数のピアスイッチが存在する場合、どのスイッチが検出メソッドを使用して、どのアクセスポイントの検出をするか制御することができます。

あるアクセスポイントの検出をある特定のスイッチから行う場合は、以下の方法のうち、いずれか一つを実行します。

- すべてのスイッチでレイヤ 2 検出を無効にし、1 台の統合スイッチにのみ検出するアクセスポイントの IP アドレスを登録する。
- アクセスポイントに 1 台の統合スイッチの IP アドレスのみを登録する。
- DHCP オプション 43 に 1 台の統合スイッチの IP アドレスのみを登録する。

さらに他の方法として、RADIUS サーバがアクセスポイント認証プロセスでアクセスポイントの MAC アドレスを確認中に、スイッチの IP アドレスをリプライさせる方法もあります。RADIUS サーバにスイッチの IP アドレスをリプライさせる設定方法については、141 ページの「付録 B 外部 RADIUS サーバの設定」を参照してください。

RADIUS サーバが、管理対象として有効なアクセスポイントであると認識し、スイッチと異なる IP アドレスをリプライすると、このスイッチは re-link メッセージに、このアクセスポイントが接続を行うべきスイッチの IP アドレスを付与して、アクセスポイントに送信します。アクセスポイントは re-link メッセージを受け取ると、そのスイッチの IP アドレスを登録して、前のスイッチとの TCP 接続を切断し、新規に検出プロセスを開始します。

ピアグループ内の 4 つのスイッチのうち、どのスイッチからでもアクセスポイントの管理を行えるように、D-Link 統合アクセスシステムを設定することも可能です。あるアクセスポイントを管理する統合スイッチがダウンした場合、他のバックアップスイッチに管理を引き継がせることも可能です。

1 台または複数のピアスイッチをアクセスポイント管理のバックアップスイッチにしたい場合は、以下のうち、いずれか一つの検出方法を実行してください。

- アクセスポイントといずれかのピアスイッチが同一のレイヤ 2 ブロードキャストドメインに属しており、レイヤ 2 検出が有効に設定されていて、すべてのデバイスがデフォルト VLAN 設定されている場合、プライマリ統合スイッチが接続不能に陥った際には、ピアスイッチが自動的にアクセスポイントを検出します。
- アクセスポイントの IP アドレスをスイッチ（最高 4 台）に登録する。
- アクセスポイントの CLI に接続し、スイッチ（最高 4 台）の IP アドレスを登録する。
- DHCP オプション 43 にピアグループのスイッチ（最高 4 台）の IP アドレスを登録する。

スイッチと管理対象のアクセスポイントへの IP アドレスの割り当て

D-Link 統合スイッチは、スイッチ同士、または D-Link アクセスポイントとの間で IP プロトコルを使用して通信をします。そのため、各デバイスは有効な IP アドレスを持つ必要があります。

ルーティング機能を無効にした D-Link 統合スイッチ

D-Link 統合スイッチのルーティングモードが無効の場合、スイッチは初期設定中に登録したネットワークインタフェースアドレスを使用します。

注意 ネットワークインタフェースの IP アドレスを変更すると、スイッチの無線機能は自動的に一度無効になり、再度有効になります。IP アドレスの割り当てに DHCP 機能を使用した場合はリース期間の失効にご注意ください。

ルーティング機能を有効にした D-Link 統合スイッチ

D-Link 統合スイッチ上でルーティングモードが有効になっている場合、そのスイッチには、ループバックインタフェース、またはルーティングインタフェースを定義しておく必要があります。ピアスイッチとアクセスポイントは、スイッチの認識およびスイッチとの通信をするために、最小のインデックスを持つループバックインタフェースの IP アドレスを使用します。ループバックインタフェースを定義していない場合は、無線機能は最小のインデックスを持つルーティングインタフェースを使用します。

ルーティング機能を有効にしている場合は、ループバックインタフェースを定義することを強くお勧めします。ループバックインタフェースを定義することにより、複数のルーティングインタフェースが存在する場合に、無線機能の IP アドレスとしてどのルーティングインタフェースを使用するかを指定することができます。これにより、統合スイッチの IP アドレスを使用する検出モード時のトラブルを回避することができます。ループバックインタフェースを使用すれば、無線機能用の IP アドレスとして常に同じものを使用できます。

注意 上のループバックインタフェースとは、自分自身を示す IP アドレス 127.0.0.1 を持つループバックインタフェースとは異なります。スイッチの無線インタフェースとしてループバックインタフェースを設定する際は、それが永続的な論理インタフェースであり、IP アドレス 127.0.0.1 ではないということが重要になります。ループバックインタフェースには専用のサブネットを設け、ネットワーク中の他のデバイスはループバックインタフェースにアクセス可能である必要があります。

ループバックインタフェースを定義することの利点は、ループバックインタフェースはダウンしないという点にあります。反対に欠点は、ネットワーク構成が複雑になることです。これはループバックインタフェースは自分自身のサブネットに属し、ネットワークの他のデバイスはそのサブネットまでの到達方法を知っている必要があるためです。
ネットワーク中の統合スイッチと管理対象のアクセスポイント間には、ルートが必要です。アクセスポイントから統合スイッチの無線インタフェースに指定された IP アドレスへの ping 送信が可能である必要があります。スイッチにスタティックルートを設定するためには、ナビゲーションメニューで **LAN タブ > L3 Features > Router** の順にメニューをクリックし、表示される設定ページを使用します。

以下の手順では、CLI にてルーティング機能を有効にし、ルーティングインタフェースまたはループバックインタフェースの IP アドレスを設定する例を示します。

1. CLI にログインし、Global Config モードに遷移します。

```
(switch-prompt)
User:admin
Password:
(switch-prompt) >enable
Password:
(switch-prompt) #config
(switch-prompt) (Config)#
```

2. ルーティング機能を有効にします。

```
(switch-prompt) (Config)#ip routing
```

3. ループバックインタフェース 0 の Interface Config mode に移行し、IP アドレスとサブネットマスクを登録します。

```
(switch-prompt) (Config)#interface loopback 0
(switch-prompt) (Interface loopback 0)#ip address 10.1.1.1 255.255.0.0
```

4. [この設定は必要に応じて行います] スロット 0 ポート 2 の Interface Config mode に移行し、IP アドレスとサブネットマスクを登録し、インタフェースのルーティング機能を有効にします。

```
(switch-prompt) (Config)#interface 0/2
(switch-prompt) (Interface 0/2)#ip address 192.168.1.24 255.255.255.0
(switch-prompt) (Interface 0/2)#routing
```

CLI の他にも、Web インタフェースや SNMP を使用し、ルーティング情報の有効化や IP アドレスの設定を行うことができます。以下に、Web インタフェースを使用して、スイッチ上でルーティング情報を有効にし、IP アドレスの設定をする方法を示します。

注意 ルーティング機能の設定はナビゲーションメニュー内の「LAN」タブを使用して行います。

1. Web インタフェースにログインし、**LAN タブ > L3 Features > IP > Configuration** の順にメニューをクリックして以下の画面を表示します。

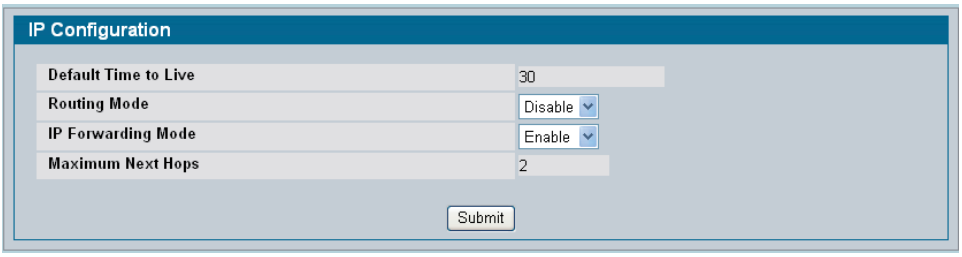


図 4-7 IP Configuration 画面

2. 「Routing Mode」プルダウンメニューから「Enable」を選択し「Submit」ボタンをクリックします。

3. ループバックインタフェースを作成するためには、**L3 Features > Loopbacks > Configuration** の順にメニューをクリックし、「Loop Back Configuration」画面を表示します。

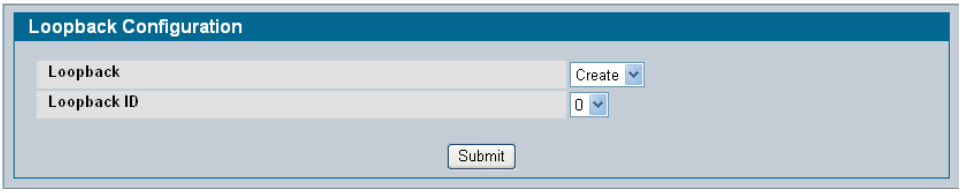


図 4-8 Loop Back Configuration 画面

4. 「Loopback」プルダウンメニューから「Create」を選択し「Submit」ボタンをクリックします。

5. IPv4 アドレスとサブネットマスクをそれぞれの欄に入力し、「Submit」ボタンをクリックします。

6. ルーティングインタフェースを作成し、IP アドレスを割り付けるには、**L3 Features > IP > Interface Configuration** の順にメニューをクリックし、「IP Interface Configuration」画面を表示します。「Slot/Port」プルダウンメニューから設定を行うインタフェースを選択します。

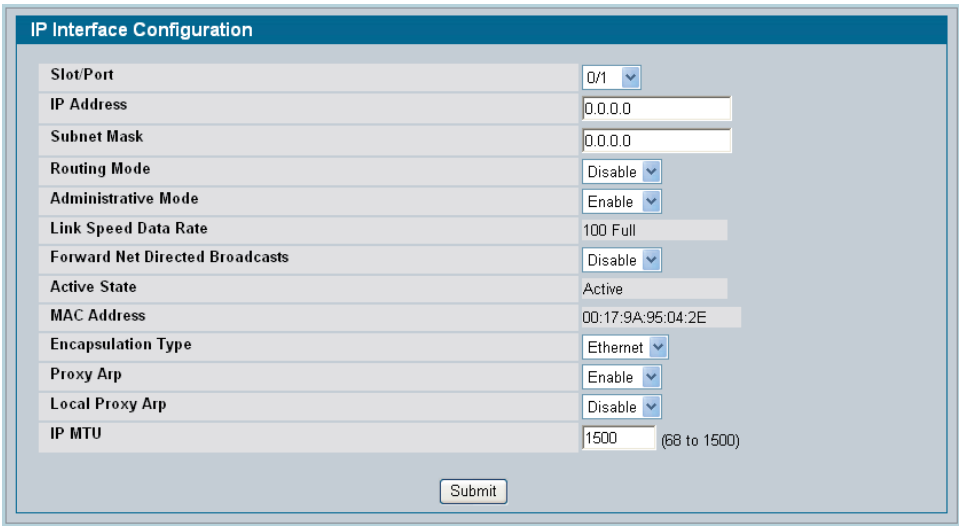


図 4-9 IP Interface Configuration 画面

7. IPv4 アドレスとサブネットマスクをそれぞれの欄に入力し、「Routing Mode」プルダウンメニューから「Enable」を選択し、「Submit」ボタンをクリックします。

D-Link アクセスポイント

D-Link アクセスポイントでは、IP アドレスの初期値は 10.90.90.91/8 で、DHCP 機能は初期値で有効となっています。ご使用のネットワーク上に DHCP サーバが存在しない場合、アクセスポイントはスタティック IP アドレスを割り当てられるまで、初期値の IP アドレスを保持します。

AP のデフォルト IP アドレスに Telnet することにより、10.0.0.0/8 のネットワーク上のホストから AP の CLI に接続できます。

アクセスポイントへのスタティック IP アドレスの設定は、以下の手順に従って行います。

1. D-Link アクセスポイントにログインします。
   アクセスポイントへのログインの方法は、34 ページの「アクセスポイントへのログイン」を参照してください。

2. **get management** コマンドを実行し、アクセスポイントの管理用インタフェースについての情報を確認します。

3. アクセスポイント上の DHCP クライアントを無効にし、DHCP Request をブロードキャストしないようにします。

   ```
   set management dhcp-status down
   ```

4. 以下のコマンドを実行して、スタティック IP アドレスを設定します。

   ```
   set management static-ip <IP アドレス > static-mask < サブネットマスク >
   コマンド入力例 : set management static-ip 192.168.22.133 static-mask 255.255.255.0
   ```

5. 以下のコマンドを実行して、デフォルトゲートウェイを設定します。

   ```
   set static-ip-route gateway < ゲートウェイ IP アドレス > mask < サブネット >
   コマンド入力例 : set static-ip-route gateway 10.254.24.1 mask 255.255.248.0
   ```

6. **save-running** コマンドを実行し、設定をメモリに保存します。

統合スイッチを DHCP サーバとして使用することも可能です。統合スイッチをアクセスポイントからの DHCP Request に応答する DHCP サーバとして使用する場合は、46 ページの「DHCP オプションにスイッチ情報を設定する」を参照してください。

アクセスポイントとピアスイッチ検出機能を有効にする

D-Link 統合スイッチはピアスイッチや D-Link アクセスポイントを検出します。検出は、それらのデバイスが互いに接続しているか、同じレイヤ 2 ブロードキャストドメインに存在しているか、または異なる IP サブネットに属しているかなどに関係なく行われます。

D-Link アクセスポイントと統合スイッチ間の検出機能は、以下の方法のいずれかにより有効にできます。

- D-Link 無線デバイス検出プロトコルのブロードキャストに VLAN を使用する。
- アクセスポイントの CLI に接続し、スイッチの IP アドレスを手動で登録する。
- アクセスポイントからの DHCP Client Request に応答する DHCP Response 内にスイッチの IP アドレスを含むように、DHCP サーバに設定をする。
- アクセスポイントの IP アドレスを手動でスイッチに登録する。複数のピアスイッチが同じアクセスポイントを検出することがありますが、最初の接続が優先されます。

一度スイッチとの接続が確立されると、アクセスポイントはその接続が切れるまで、または相手スイッチから一度切断し、他のスイッチと接続するように指示されるまで接続を持続させます。

以下の項に、各検出メカニズムについて説明します。

D-Link 無線デバイス検出プロトコル

D-Link 統合スイッチとアクセスポイントが同一レイヤ 2 マルチキャストドメインに存在している場合、無線デバイス検出プロトコルはとても有効な検出プロトコルであると言えます。統合スイッチはデバイス検出が有効に設定されている各 VLAN に、定期的に Discovery メッセージを含むマルチキャストパケットを送信します。最大 16 の VLAN 上で検出プロトコルを有効にすることができます。

デフォルトでは、VLAN 1 はアクセスポイント上で有効にされ、統合スイッチを検出する設定になっています。スイッチとアクセスポイントが同じレイヤ 2 マルチキャストドメインに存在している場合、アクセスポイントがスイッチを検出するための設定は必要ありません。

スイッチがレイヤ 2 検出機能によって新しいアクセスポイントを検出したが、そのアクセスポイントの MAC アドレスが Valid AP データベースに存在しなかった場合、そのアクセスポイントは、WLAN タブの **Monitoring > Access Point** をクリックして表示できる「Authentication Failed Access Points」画面に表示されます。CLI を使用して認証に失敗したアクセスポイントを確認するためには、管理者モード (Privilege EXEC モード) にて、「**`show wireless ap failure status`**」コマンドを実行します。

アクセスポイントは、管理用 VLAN からの Discovery メッセージのみを処理します。また、アクセスポイントは無線メディアへの Discovery メッセージ転送は行いません。
以下の手順で、Web インタフェースを使用して VLAN を検出リストに登録します。

1. ブラウザから D-Link 統合スイッチにログインします。
2. ナビゲーションメニューから、**WLAN タブ > Administration > Basic Setup** の順にメニューをクリックし、さらに「Discovery」タブを選択します。
3. 「L2/VLAN Discovery」ボックスにチェックが入っていることを確認し、アクセスポイントまたはピアスイッチの管理用 VLAN ID を入力します。
4. 「Add」ボタンをクリックして VLAN をリストに追加します。

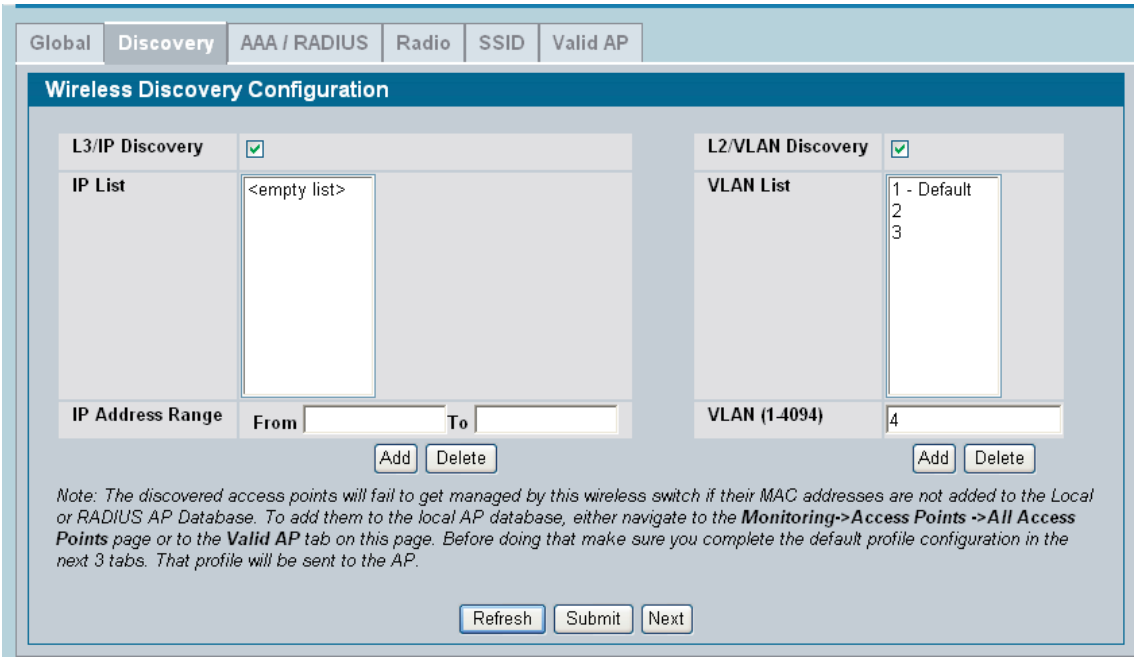

Global
Discovery
AAA / RADIUS
Radio
SSID
Valid AP
Wireless Discovery Configuration
L3/IP Discovery
IP List
<empty list>
IP Address Range
From
To
Add
Delete
L2/VLAN Discovery
VLAN List
1 - Default
2
3
VLAN (1-4094)
4
Add
Delete
Note: The discovered access points will fail to get managed by this wireless switch if their MAC addresses are not added to the Local or RADIUS AP Database. To add them to the local AP database, either navigate to the Monitoring->Access Points ->All Access Points page or to the Valid AP tab on this page. Before doing that make sure you complete the default profile configuration in the next 3 tabs. That profile will be sent to the AP.
Refresh
Submit
Next

図 4-10　VLAN を Web インタフェースで検出リストに追加にする

5. 「Submit」ボタンをクリックして変更を適用します。

統合スイッチからデバイス検出状況を確認することができます。スイッチ側からアクセスポイントの検出状況を確認するためには、**WLAN タブ > Monitoring > Access Point > Managed Access Points** の順にメニューをクリックします。もし、アクセスポイントの MAC アドレスをローカルデータベースまたは RADIUS Valid AP データベースに登録していない場合は、アクセスポイントは **WLAN タブ > Monitoring > Access Point > Authentication Failed Access Points** の順にメニューをクリックして表示される「Authentication Failed Access Points」リスト上に表示されます。認証失敗原因として「No Database Entry」と表示されます。アクセスポイント認証の詳細については 48 ページの「4.6 アクセスポイントの認証」を参照してください。

以下に、CLI を使用して VLAN をリストに登録する例を紹介します。

1. Telnet、SSH またはシリアル接続により D-Link 統合スイッチにログインし、Wireless Configuration モードに遷移します。

```
(switch-prompt) >enable
Password:
(switch-prompt) #config
(switch-prompt) (Config)#wireless
```

2. VLAN を検出リストに登録します。

```
(switch-prompt) (Config-wireless)#discovery vlan-list 4
```

3. 「Ctrl」キーと「Z」を同時に押下し、管理者モード（Privilege EXEC モード）に戻ります。

4. 設定をコンフィグレーションファイルに保存します。

```
(switch-prompt) #write

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n)y

Configuration Saved!
```

アクセスポイントの管理状況を確認するためには、以下のコマンドを実行してください。

```
(switch-prompt) #show wireless ap status
```

スイッチにピアスイッチとアクセスポイントの IP アドレスを登録する

D-Link 統合スイッチには、ピアスイッチとアクセスポイント用の 256 件までの IP アドレスを登録できます。スイッチは、このリストに登録されているすべての IP アドレスに対して association invitation を送信します。デバイスがこの invitation を受け取り、スイッチによる認証にパスすると、スイッチとアクセスポイント / ピアスイッチは接続を開始します。

この検出方法は、検出するデバイスが異なるサブネットに属する場合に便利です。実際、スイッチが異なるサブネット内のピアを認識するためには、ピアのレイヤ 3 検出リストに各スイッチの IP アドレスを登録する必要があります。

注意 IP アドレスリストは管理対象 Valid AP リストとは異なります。本リストにより検出されたデバイスが有効なアクセスポイントやスイッチではない場合があります。

注意 アクセスポイントが、既に他の方法によって検出されている場合は、統合スイッチはそのアクセスポイントの IP アドレスに対してポーリングを行いません。

表 4-4　L3/IP 検出

設定項目	説明
L3/IP Discovery	アクセスポイントおよびピアスイッチの IP ベースの検出を有効または無効にします。チェックすると IP ポーリングが有効になり、スイッチは IP リスト中の各アドレスに対して定期的に呼び出しを行います。初期値は有効です。
IP List	検出用に登録された IP アドレスのリストです。リストからエントリを削除するためには、対応するエントリを選択して「Delete」ボタンをクリックします。デフォルトのエントリはありません。256 件までのエントリをサポートします。
IP Address Range	「IP List」に登録する IP アドレスの範囲を入力します。「From」欄にアドレス範囲で最小のものを入力し、「To」欄に範囲で最大のアドレスを入力して「Add」ボタンをクリックします。指定した範囲内のすべてのアドレスが「IP List」に追加されます。必要なアドレスの追加後、「Submit」ボタンをクリックしてコンフィグレーションに保存します。 **注意** 1 件の IP アドレスを登録する場合は、「From」欄にのみ入力し、「To」欄は空白のままにして、「Add」ボタンをクリックします。

アクセスポイントの IP アドレスを確認するためには、34 ページの「アクセスポイントへのログイン」を参考にしてアクセスポイントにログインし、**get management** コマンドを実行してください。

以下の手順で Web インタフェースを使用して、ピアスイッチやアクセスポイントの IP アドレスを検出リストに登録します。

1. Web ブラウザから D-Link 統合スイッチにログインします。
2. **WLAN タブ > Administration > Basic Setup** の順にメニューをクリックし「Discovery」タブを選択します。
3. 「L2/VLAN Discovery」ボックスのチェックを外し、スイッチが L2 検出メッセージを送信しないようにします。
4. 「L3/IP Discovery」ボックスにチェックを入れて、ピアスイッチまたはアクセスポイントの IP アドレス範囲を「From」/「To」欄で指定します。連続していない IP アドレスや、1 件のみの登録の場合は、「From」欄のみ入力し、「To」欄は空欄にしておきます。
5. 「Add」ボタンをクリックし、リストに IP アドレスを追加します。
6. 「Submit」ボタンをクリックし、変更をスイッチに適用します。

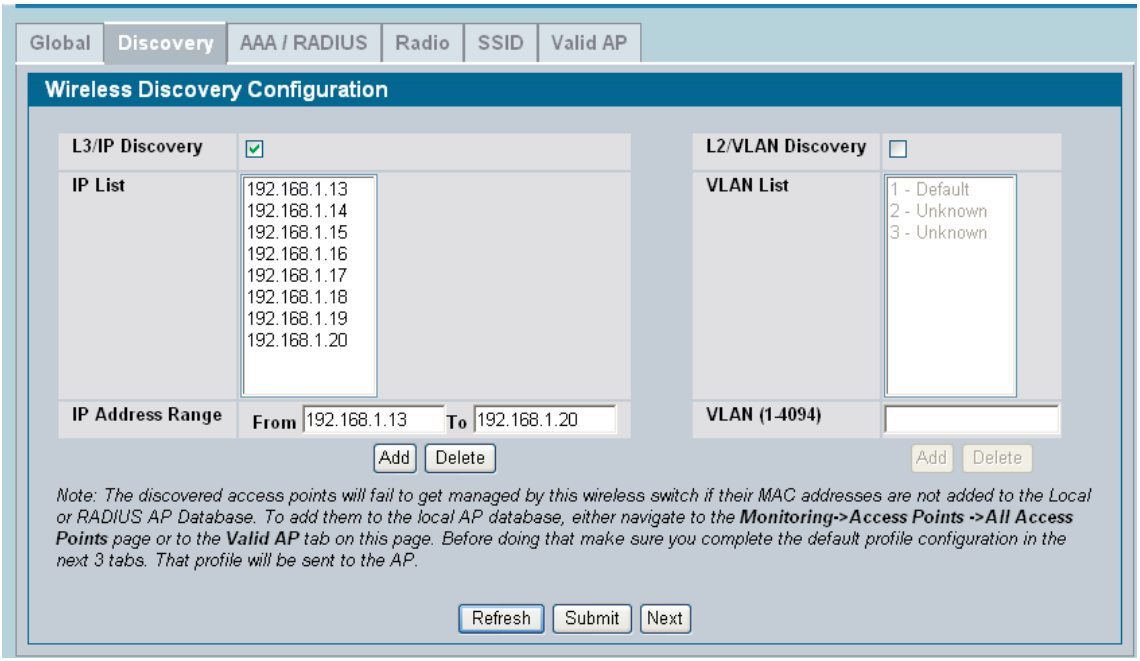


図 4-11　IP アドレスを Web インタフェースで検出リストに登録にする

スイッチが登録した IP アドレスに対して正しく呼び出しを行っていることを確認するためには、**WLAN タブ > Monitoring > Global** の順にメニューをクリックして「IP Discovery」タブを表示します。

以下に、CLI によって L3 検出リストにアドレスを登録する方法の例を示します。

1. Telnet、SSH またはシリアル接続により D-Link 統合スイッチにログインし、Wireless Configuration モードに遷移します。

```
(switch-prompt) >enable
Password:
(switch-prompt) #config
(switch-prompt) (Config)#wireless
```

2. ピアスイッチかアクセスポイントの IP アドレスを検出リストに追加します。

```
(switch-prompt) (Config-wireless)#discovery ip-list 192.168.6.211
```

CLI では 1 回に 1 件のアドレスしか登録できません。

3. 「Ctrl」キーと「Z」を同時に押下し、Privilege EXEC モードに戻ります。
4. 設定をコンフィグレーションファイルに保存します。

```
(switch-prompt) #write

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n)y

Configuration Saved!
```

管理対象のアクセスポイントの情報を確認するためには、以下のコマンドを実行します。

```
(switch-prompt) #show wireless ap status
```

D-Link アクセスポイントにスイッチの IP アドレスを登録する

D-Link アクセスポイントの CLI に接続して、D-Link 統合スイッチの IP アドレスまたは DNS 名を静的に登録することができます。

アクセスポイントと接続する D-Link 統合スイッチは 4 台まで登録可能ですが、アクセスポイントを管理するスイッチは 1 台のみです。他の 3 台はバックアップ用または交換用として使用します。

アクセスポイントに、スイッチの IP アドレスまたは DNS 名を登録すると、そのアクセスポイントはそれらのスイッチとだけ接続を行います。もし他のスイッチが、他のメカニズムによってアクセスポイントを検出しても、アクセスポイントは登録を行ったスイッチからの接続のみを受け入れます。アクセスポイントを管理するスイッチの IP アドレスを変更する場合は、セカンダリスイッチに管理を委任する必要があります。そのためには、アクセスポイントの CLI に直接接続し、管理を行うスイッチの IP アドアレスを登録します。

D-Link アクセスポイントの IP アドレスを知っている場合は、Telnet で CLI に接続できます。アクセスポイントの IP アドレスの初期値は 10.90.90.91 サブネットマスクの初期値は 255.0.0.0 です。

注意 この方法を使う場合には、アクセスポイントが統合スイッチへのルートを知っている必要があります。

1. D-Link アクセスポイントにログインします。
   アクセスポイントにログインする方法については、34 ページの「アクセスポイントへのログイン」を参照してください。

2. アクセスポイントの管理に使用できる 4 台までのスイッチの IP アドレスを登録します。
   例として、IP アドレス 192.168.66.202 の統合スイッチと 192.168.19.242 の統合スイッチの 2 台を登録します。

```
WLAN-AP#set managed-ap switch-address-1 192.168.66.202
WLAN-AP#set managed-ap switch-address-2 192.168.19.242
```

3. **get managed-ap** コマンドを実行して、登録した情報を確認します。

```
WLAN-AP#get managed-ap
Property                Value
------------------------------------------------
mode                    up
ap-state                down
switch-address-1        192.168.66.202
switch-address-2        192.168.19.242
switch-address-3
switch-address-4
dhcp-switch-address-1
dhcp-switch-address-2
dhcp-switch-address-3
dhcp-switch-address-4
managed-mode-watchdog   0
```

統合スイッチから検出状況を確認することができます。スイッチがアクセスポイントの検出を行ったか否かを確認するためには、**WLAN タブ > Monitoring > Access Point > Mnaged Access Points** の順にメニューをクリックします。アクセスポイントによるスイッチ検出には数分かかる場合があります。

注意 アクセスポイントの MAC アドレスをローカルまたは RADIUS Valid AP データベースに登録していない場合は、アクセスポイントは **Monitoring > Access Point > Authentication Failed Access Points** 画面に表示されます。認証失敗原因として「No Database Entry」と表示されます。アクセスポイント認証の詳細については 48 ページの「4.6 アクセスポイントの認証」を参照してください。

管理対象のアクセスポイントの状況を統合スイッチの CLI によって確認するためには、以下のコマンドを実行してください。

```
(switch-prompt) #show wireless ap status
```

DHCP オプションにスイッチ情報を設定する

アクセスポイントにスイッチの IP アドレスを静的に設定する代わりに、4 台までの D-Link 統合スイッチの IP アドレスを DHCP オプション 43 内に格納して、ネットワーク上の DHCP サーバからアクセスポイントに送信する方法もあります。既に D-Link アクセスポイントにスタティック IP アドレスが設定されている場合は、DHCP オプション 43 は無視されます。

DHCP サーバに DHCP オプションを登録する方法は、お使用の DHCP サーバによって異なります。Microsoft Windows 2000 または 2003 で DHCP サーバをご使用であれば、以下の手順に従って、アクセスポイントへの DHCP オプション 43 に使用するスコープを作成します。

1. Windows の「コントロールパネル」で「管理ツール」アイコンをクリックし、「管理ツール」画面を表示します。

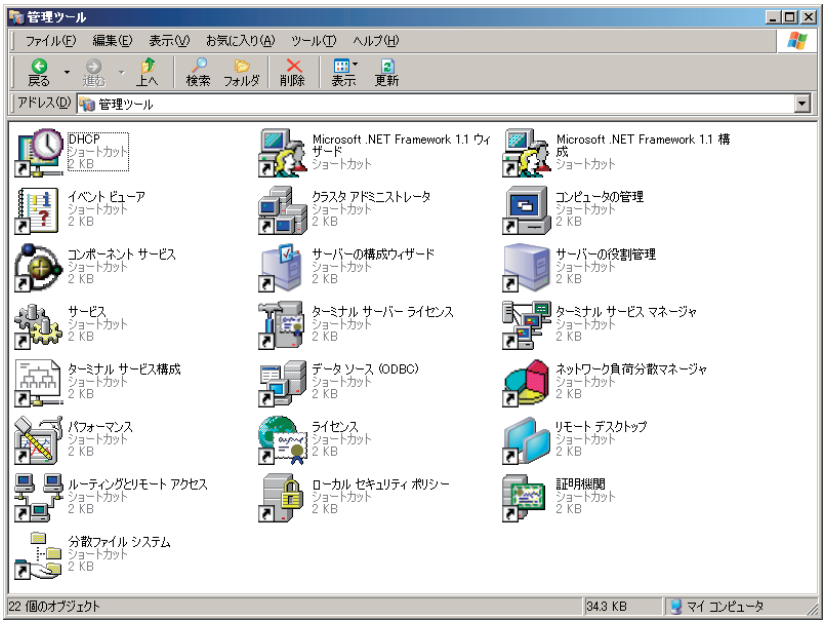


図 4-12 「管理ツール」画面

2. 「DHCP」アイコンをクリックし、DHCP マネージャを起動します。

図 4-13 DHCP マネージャ画面

3. DHCP マネージャで、目的のスコープの「スコープオプション」を右クリックし、「オプションの構成」を選択します。

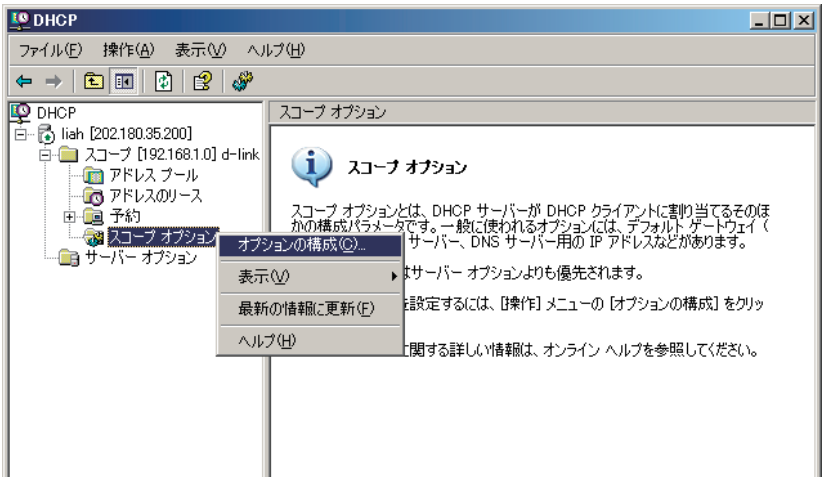


図 4-14 Windows の DHCP サーバ設定画面 1

4. 「スコープオプション」の「全般」タブ内の利用可能なオプションリストをスクロールし、「043 ベンダ固有情報」ボックスにチェックを入れます。

5. オプション 43 データを「データ入力」欄に入力します。
DHCP オプション 43 のデータフォーマットは、RFC 2132 で規定されています。192.168.1.10 の IP アドレスをバイナリコラムに入力するためには、データタイプコード（01）、アドレス長（04）、次に 16 進数表記で IP アドレスを入力します。その後も登録するアドレスのごとに、データタイプ、アドレス長、16 進数の IP アドレスの順で入力を続けます。

例えば、4 つの IP アドレス（192.168.1.10、192.168.2.10、192.168.3.10、192.168.4.16）をオプション 43 に登録する場合、データエントリ欄に以下の 16 進数コードを入力します。

```
01 04 0C A8 01 0A 01 04 0C A8 02 0A 01 04 0C A8 03 0A 01 04 0C A8 04 10
```

以下の図は、Windows DHCP サーバのデータエントリ欄に 4 件の IP アドレスを入力した状態を示しています。

図 4-15　Windows の DHCP サーバ設定画面 2

6. 「OK」ボタンをクリックします。
以下の図は、オプション 43 の設定を行ったスコープを示しています。

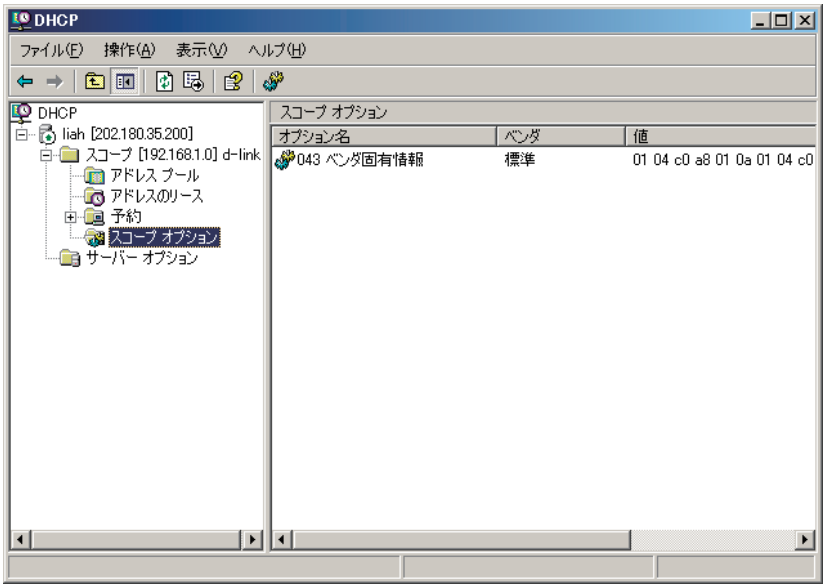


図 4-16　Windows の DHCP サーバ設定画面 3

4.6 アクセスポイントの認証

D-Link 統合スイッチがアクセスポイントを管理するためには、アクセスポイントの MAC アドレスをローカルデータベースまたは外部 RADIUS データベースに登録する必要があります。

スイッチが他の統合スイッチの管理下にないアクセスポイントを検出した時、ローカルまたは RADIUS の Valid AP データベースで MAC アドレスを検索します。データベースにそのアクセスポイントの MAC アドレスが存在すれば、スイッチはアクセスポイントの認証を行い、自分の管理対象とします。データベースに MAC アドレスの登録をしていないアクセスポイントは「Authentication Failed Access Points」リスト上に表示され、認証失敗原因として「No Database Entry」が表示されます。

オプションとして、統合スイッチがアクセスポイントの管理をする前に、アクセスポイントの認証をすることも可能です。アクセスポイントの MAC アドレスをローカルデータベースまたは RADIUS データベースに登録する際に、認証情報も登録することができます。認証を有効に設定すると、スイッチがアクセスポイントを認知した直後に認証を行います。

注意 スイッチがアクセスポイントの認知に成功すると、そのアクセスポイントに AP プロファイルを送信します。AP プロファイルには、無線設定、セキュリティ、SSID などのアクセスポイントに定義されたすべての設定情報が含まれています。デフォルト AP プロファイルの設定については、54 ページの「第 5 章 アクセスポイントの設定」を参照してください。

アクセスポイント認証の設定

無線ネットワークへのアクセスに対するセキュリティに IEEE 802.1X 認証または他のセキュリティ方式が採用されていない場合、アクセスポイントが常に認証を用いて不正アクセスポイントが自動的にスイッチと接続を行わないようにする必要があります。

アクセスポイントでスイッチに接続するために自身の認証を行うためには、以下の手順で設定を行います。

1. 本項に示した方法により、スイッチ側でアクセスポイント認証を有効にします。
2. アクセスポイントの CLI に接続し、34 ページの「4.4 アクセスポイント側の準備」の方法に従ってパスフレーズを登録します。
3. Valid AP データベースにパスフレーズを登録します。
   ローカルデータベースにパスフレーズを登録する方法については、49 ページの「アクセスポイント認証にローカルデータベースを使用する」を参照してください。RADIUS データベースにパスフレーズを登録する方法については、51 ページの「アクセスポイント認証に RADIUS データベースを使用する」を参照してください。

統合スイッチ側でアクセスポイント認証を有効にするためには、**WLAN タブ > Administration > Basic Setup** をクリックして「Global」タブを開きます。「AP Authentication」ボックスにチェックを入れて、「Submit」ボタンをクリックし、変更を適用します。

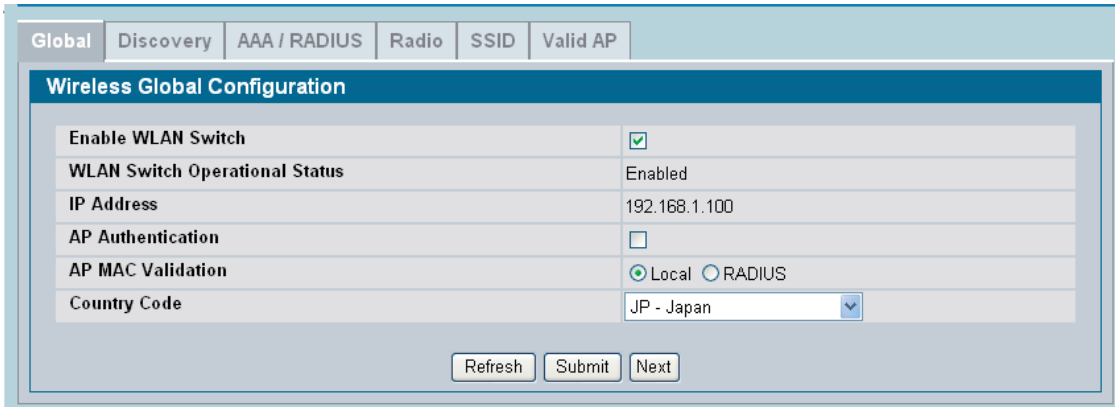


図 4-17　アクセスポイント認証を有効にする

CLI によりアクセスポイント認証を有効にするためには、「Wireless Config」モードに遷移して、以下のように設定を行います。

```
(switch-prompt) >enable
Password:
(switch-prompt) #config
(switch-prompt) (Config)#wireless
(switch-prompt) (Config-wireless)#ap authentication
```

アクセスポイント認証にローカルデータベースを使用する

ローカル Valid AP データベースを使用するためには、「AP MAC Validation」欄で「Local」を選択し、データベースにアクセスポイントの情報を登録します。これらの設定はすべてスイッチで行います。

アクセスポイント認証のためのローカルデータベース設定は、以下の手順で行ってください。

1. **WLAN タブ > Administration > Basic Setup** の順にメニューをクリックして「Global」タブを開きます。「AP MAC Validation」欄で「Local」が選択されていることを確認します（Local はデフォルト設定です）。

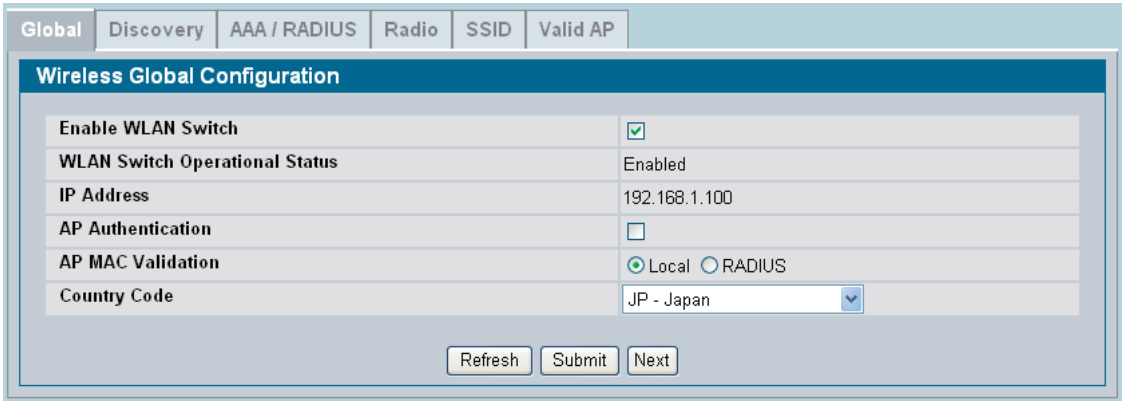


図 4-18　Wireless Global Configuration 画面

2. 設定の変更を行った場合は「Submit」ボタンをクリックします。

3. 「Valid AP」タブを開きます。

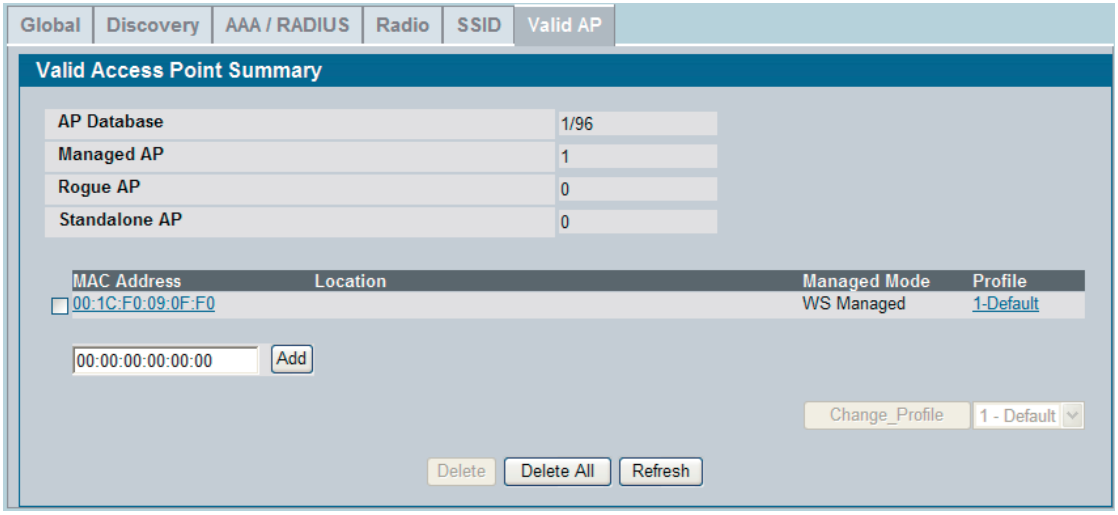


図 4-19　アクセスポイント認証を有効にする

4. 「MAC Address」欄に認証するアクセスポイントの MAC アドレスを入力後、「Location」欄にアクセスポイントのあるロケーションを入力し、「Add」ボタンをクリックします。

注意 スイッチがアクセスポイントを検出済みの場合、その MAC アドレスは「Monitoring」から「Access Point」をクリックした配下の「Managed Access Points」ページに表示されます。または、「Monitoring」から「Access Point」をクリックした配下の「Authentication Failed Access Points」ページに表示されます。CLI を使用して検出したアクセスポイントの MAC アドレスを確認するためには、Privilege EXEC モードにて **`show wireless ap status`** コマンド、または **`show wireless ap failure status`** コマンドを実行します。

アクセスポイントを追加すると、新しい項目が表示され、パスフレーズなどのアクセスポイントの認証情報が入力可能となります。

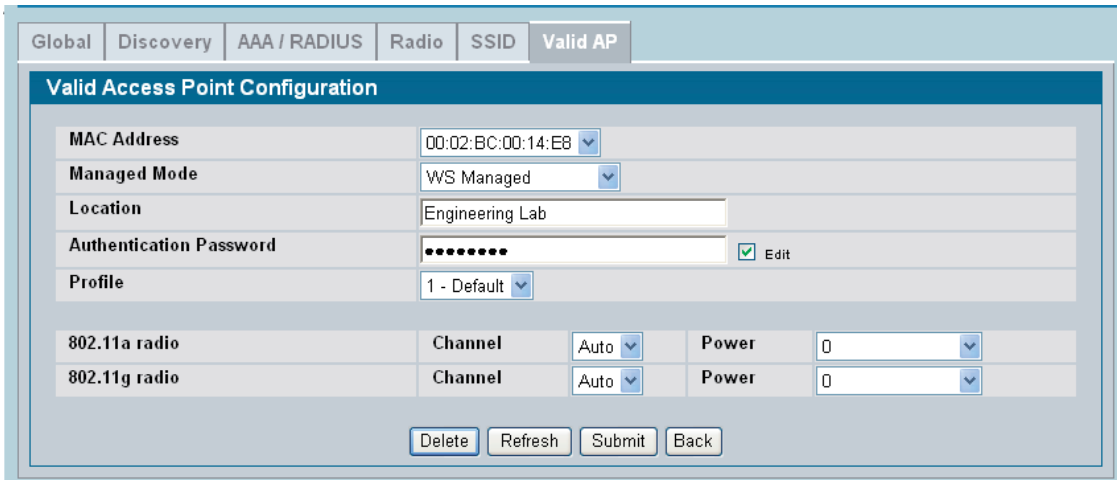


図 4-20　アクセスポイントの認証用パスワードを入力する

「Wireless Global Configuration」ページ（図 4-17）で「AP Authentication」にチェックを入れた場合は、「Edit」チェックボックスにもチェックを入れて、アクセスポイントの認証用パスワードを入力します。

5. パスワードはアクセスポイント側に登録したパスフレーズと同一である必要があります。パスワードは半角英数字 8 から 63 文字で入力します。セキュリティを強化するために、24 文字以上使用することをお勧めします。

6. アクセスポイントが使用するチャンネルや送信電力などを設定します。
「Valid Access Point Configuration」ページ（図 4-20）上の各項目についての説明や、有効アクセスポイントの設定方法については、69 ページの「5.5 Valid アクセスポイントの設定」を参照してください。

7. 「Submit」ボタンをクリックして変更内容を適用します。

次に CLI を使用したローカルデータベースの設定例を説明します。

1. スイッチにログインして、「Wireless Config」モードに入ります。

```
(switch-prompt) >enable
Password:
(switch-prompt) #config
(switch-prompt) (Config)#wireless
```

2. ローカルデータベースを認証方法として登録します。

```
(switch-prompt) (Config-wireless)#ap validation local
```

3. データベースにアクセスポイントの MAC アドレスを登録します。

```
(switch-prompt) (Config-wireless)#ap database 00:02:BC:00:14:40
```

4. アクセスポイントからスイッチ側への認証をする場合は、アクセスポイントのパスフレーズを登録します。

```
(switch-prompt) (Config-ap)#password
Enter password(8-63 characters):******************
Re-enter password:******************
```

CLI を使用して、データベースに追加のパラメータを登録する方法については、「D-Link CLI MANUAL」を参照してください。

アクセスポイント認証に RADIUS データベースを使用する

RADIUS サーバを使用してアクセスポイントを認証するためには、統合スイッチと RADIUS サーバともに設定を行う必要があります。スイッチ側では、アクセスポイント認証方法を RADIUS に設定し、IP アドレスなどの RADIUS サーバについての情報を設定します。RADIUS サーバ側では、アクセスポイント認証に使用するパスフレーズなどの Valid AP に関する設定を行います。RADIUS サーバ側での設定パラメータについては、141 ページの「付録 B 外部 RADIUS サーバの設定」を参照してください。
認証方法として、RADIUS を有効にするとローカル Valid AP データベースは使用されなくなります。ローカル Valid AP データベースはローカル認証にのみ使用されます。

RADIUS サーバを Valid AP データベースとして使用するためには、以下の手順で設定を行ってください。

1. **WLAN タブ > Administration > Basic Setup** の順にメニューをクリックし、「Global」タブを開きます。「AP MAC Validation」欄で「RADIUS」を選択します。

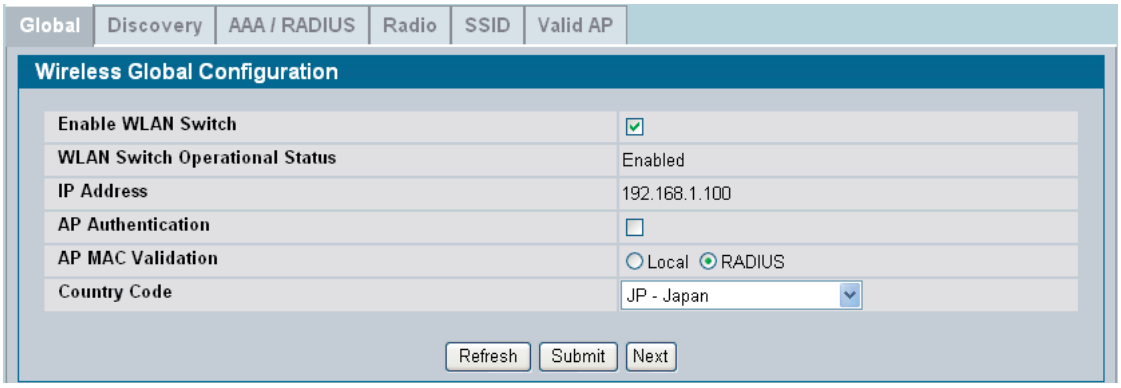


図 4-21　RADIUS サーバを使用したアクセスポイントの認証設定

「Submit」ボタンをクリックし、設定を適用します。

WLAN タブ > Administration > Basic Setup で表示される画面の「AAA/RADIUS」タブで設定する RADIUS 情報は、デフォルト AP プロファイルを使用するアクセスポイントに適用され、スイッチには適用されません。無線クライアントがアクセスポイントと接続する前に、RADIUS サーバに無線クライアントの認証をさせたい場合には、「AAA/RADIUS」タブの設定を 55 ページの「5.2 AAA と RADIUS の設定」の内容に従って行ってください。

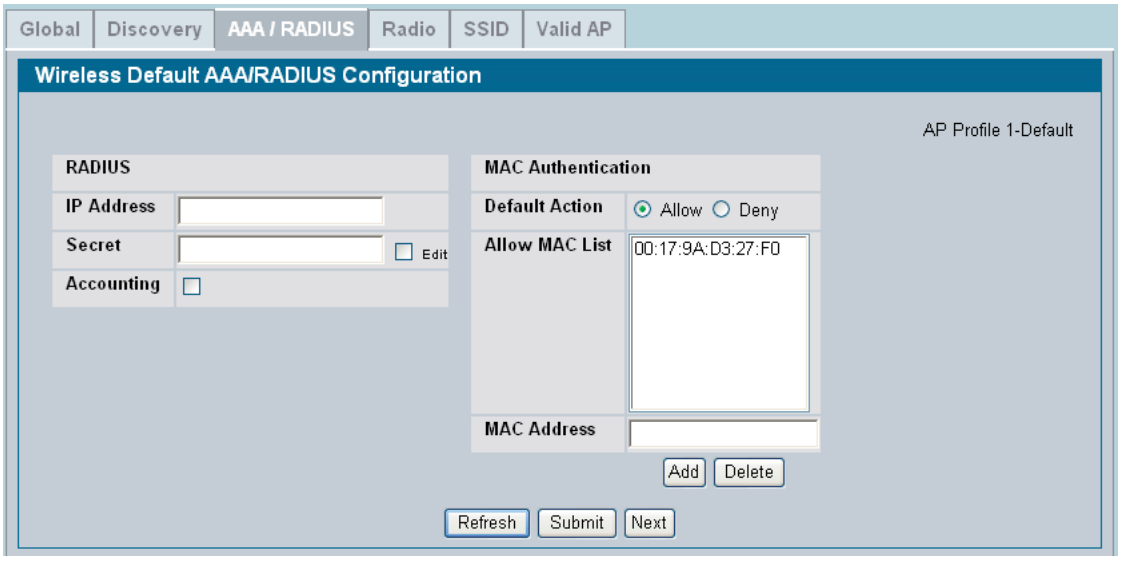


図 4-22　RADIUS サーバが認証する無線クライアントの設定

2. **LAN タブ > Security > Radius > RADIUS Authentication Server Configuration** の順にメニューをクリックします。

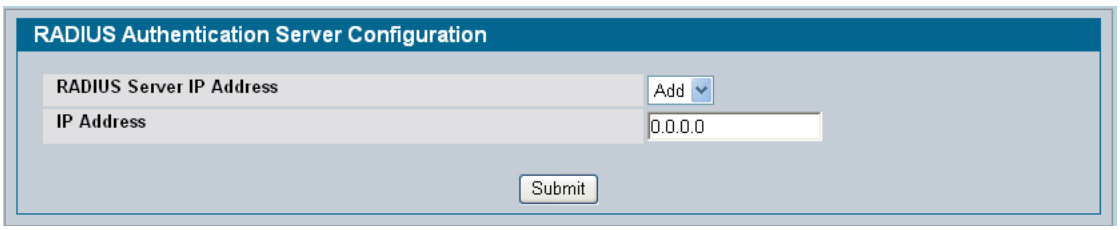


図 4-23　RADIUS サーバの IP アドレスを登録する

Valid AP データベースとして使用する RADIUS サーバの IP アドレスを入力し、「Submit」ボタンをクリックすると、新しい項目が表示されます。

3. ネットワーク上の RADIUS サーバに接続するために統合スイッチに必要な情報（共有鍵等）を設定します。

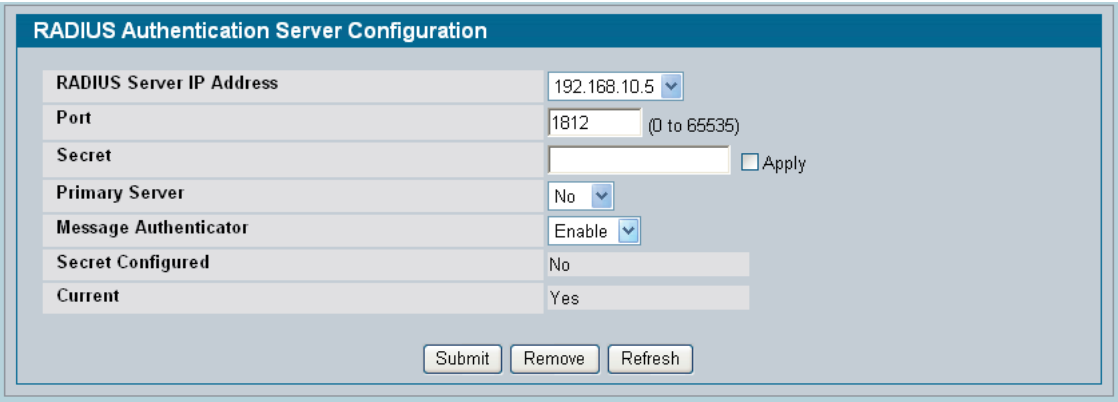


図 4-24　RADIUS サーバ用の共有鍵などを登録する

「Submit」ボタンをクリックして変更し、設定を適用します。

以下に、CLI を使用して RADIUS 認証の設定をする例を示します。

1. 「Wireless Config」モードに入ります。

```
(switch-prompt) >enable
Password:
(switch-prompt) #config
(switch-prompt) (Config)#wireless
```

2. 認証方法として RADIUS を設定します。

```
(switch-prompt) (Config-wireless)#ap validation radius
```

3. 「Global Config」モードに戻り、RADIUS サーバの設定を行います。
以下の例では、RADIUS サーバの IP アドレスは 192.168.2.2 です。

```
(switch-prompt) (Config-wireless)#exit
(switch-prompt) (Config)#radius server host auth 192.168.2.2
(switch-prompt) (Config)#radius server key auth 192.168.2.2
Enter secret(16 characters max):******************
Re-enter secret:******************
```

CLI を使用して、追加の RADIUS パラメータを登録する方法については、「D-Link CLI MANUAL」を参照してください。

認証失敗または不正アクセスポイントの管理

スイッチに接続を試みたアクセスポイントが認証に失敗したり、アクセスポイントの MAC アドレスが Valid AP データベースに登録されなかった場合、アクセスポイントの接続は許可されず、このアクセスポイントは「Authentication Failed Access Points」ページに表示されます。スイッチ側が、あるアクセスポイントがデータベースに登録されていないことを知り、またアクセスポイント側からもスイッチ検出を試みていないことが分かると、そのアクセスポイントは「Rogue/RF Scan Access」ページに表示されます。

「Authentication Failed Access Points」ページ、または「Rogue/RF Scan Access」ページに表示されているアクセスポイントを、それらのページからローカル Valid AP データベースに登録することが可能です。

以下の手順で登録を行います。

1. **WLAN タブ > Monitoring > Access Point** とクリックし、「Authentication Failed Access Points」画面、または「Rogue/RF Scan Access」画面にアクセスします。

2. 管理対象とするアクセスポイントのチェックボックスにチェックを入れて、「Manage」ボタンをクリックします。

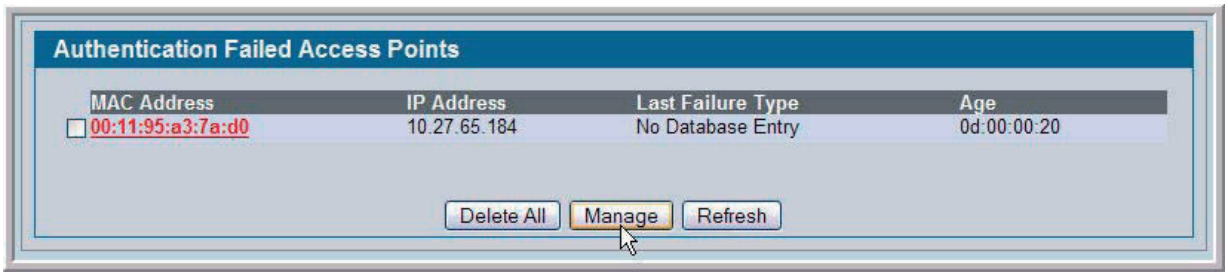


図 4-25　RADIUS サーバ用の共有鍵などを登録する

注意 「AP authentication failure」ページに表示されているアクセスポイントは、RADIUS データベースに追加できません。アクセスポイント認証に RADIUS サーバを使用する場合は、RADIUS データベースにアクセスポイントの情報を登録する必要があります。

3. 追加された AP 用に「Valid Access Point Configuration」画面が表示されます。「Location」や「Profile」などの適切なフィールドを設定し、「Submit」ボタンをクリックします。

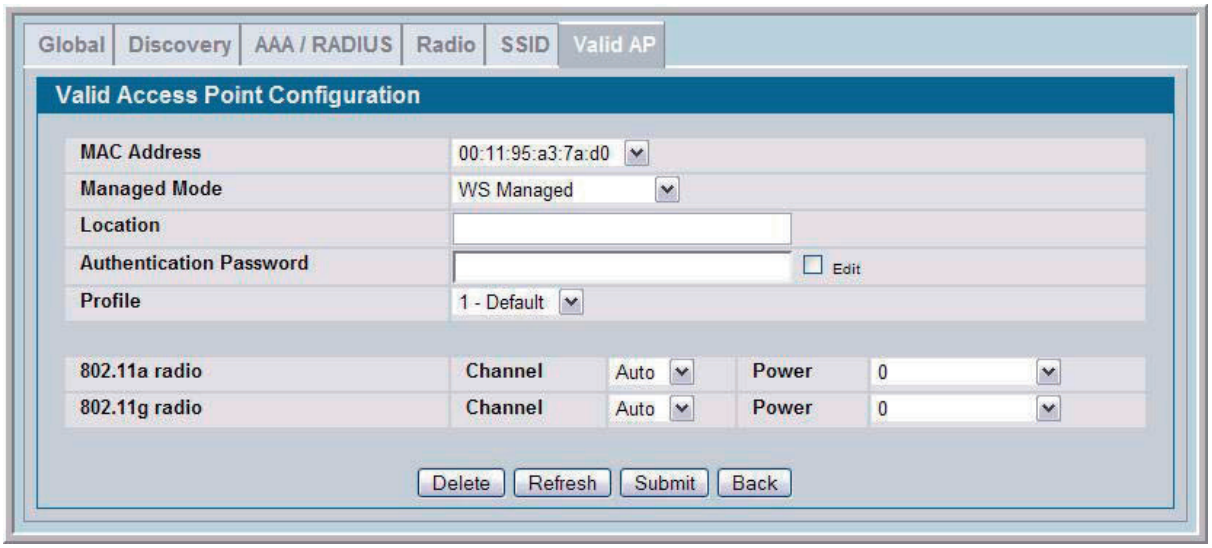


図 4-26　RADIUS サーバ用の共有鍵などを登録する

アクセスポイントは Valid AP データベース内に追加され、その MAC アドレスは、**Administration > Basic Setup > Valid AP** 画面に表示されます。

注意 管理のために複数の AP を選択する場合、設定した AP エントリを「Submit」した後に Web インタフェースは「MAC Address」欄に選択した AP をひとつずつ表示します。

CLI を使用して、認証に失敗したアクセスポイントのリストを確認するためには、Privilege EXEC モードにて **`show wireless ap failure status`** コマンドを実行します。RF スキャンにより検出されたアクセスポイントのリストを表示するためには、**`wireless ap rf-scan status`** コマンドを実行します。

ローカル Valid AP データベースに、認証に失敗したアクセスポイントや不正アクセスポイントを追加するためには、49 ページの「アクセスポイント認証にローカルデータベースを使用する」を参照してください。

第 5 章　アクセスポイントの設定

スイッチと接続する D-Link アクセスポイントを認定後、スイッチはそのアクセスポイントの管理を行います。認定の前または後に、すべてのアクセスポイントの設定をスイッチから直接行うことができます。D-Link 統合アクセスシステムは D-Link Wireless AP Protocol（DWAPP）を利用して、AP の検出、設定、管理およびモニタを行います。ここでは、アクセスポイントの設定と、D-Link 統合スイッチによるアクセスポイントの管理方法について説明します。

本章は、以下の項で構成されています。

項目	説明	参照ページ
アクセスポイントプロファイル、ネットワーク、ローカルデータベース	D-Link 統合スイッチに設定するアクセスポイントプロファイル、無線ネットワーク、およびローカルアクセスポイント・データベースについて説明します。	54 ページ
AAA と RADIUS の設定	アクセスポイントに対するクライアント認証およびアカウンティング管理に関する情報について説明します。	55 ページ
無線電波の設定	無線インタフェースを設定します。	57 ページ
SSID の設定	SSID および仮想アクセスポイント（VAP）を設定します。	61 ページ
Valid アクセスポイントの設定	各アクセスポイントにチャンネルや RF 信号送信電力レベルを指定します。また、AP モード、ローカル認証パスワード、アクセスポイントが使用するプロファイルを設定します。	69 ページ

CLI を使用してアクセスポイントを設定するコマンドについての情報は、「D-Link CLI MANUAL」を参照してください。

注意 アクセスポイントの設定変更によっては、アクセスポイントのシステム停止、また再開を引き起こすことがあります。このような場合、無線クライアントは一時的に接続できなくなります。アクセスポイントの設定は WLAN 内のトラフィックが小さい時間帯にすることをお勧めします。

5.1 アクセスポイントプロファイル、ネットワーク、ローカルデータベース

本項では、D-Link 統合スイッチに設定するアクセスポイントプロファイル、無線ネットワーク、およびローカルアクセスポイント・データベースについて説明します。

アクセスポイントプロファイル

D-Link アクセスポイントの設定は、コンフィグレーションプロファイルを使用します。プロファイルとはコンフィグレーションテンプレートのようなもので、1 台、または複数のアクセスポイントに適用することができます。D-Link 統合スイッチでは、複数のアクセスポイント用コンフィグレーションプロファイルを作成できます。アクセスポイントを確認する場合、アクセスポイントがどのプロファイルを受信するか指定します。

統合スイッチ上では多くのアクセスポイントプロファイルを定義できますが、各アクセスポイントに対して 1 つのプロファイルしか適用できません。1 つのプロファイルを複数のアクセスポイントに対して使用することも、スイッチが管理する各アクセスポイントに対してそれぞれ固有のプロファイルを作成することも可能です。既に作成済みのプロファイルとその設定内容は他のプロファイルにコピーすることや、それを元に新しいプロファイルを作成することもできます。

各プロファイルには、以下のアクセスポイント機能について独自の設定を持たせることができます。

- RADIUS サーバ設定
- MAC 認証リスト
- 無線インタフェースと RF 設定
- QoS 設定
- 仮想アクセスポイント（VAP）設定

プロファイルの変更および適用をする場合、スイッチは管理下のアクセスポイントに変更を伝え、変更後のプロファイルを使用するよう指示します。

注意 **WLAN タブ > Administration > Advanced Configuration > AP Profiles** 画面、または **`wireless ap profile apply`** コマンドを使用して、一度明確にプロファイルを適用した後は、スイッチはプロファイルの差分のみをアクセスポイントに伝えます。

更新されたプロファイルを適用するまでは、アクセスポイントは元のプロファイル設定に従って動作します。Valid AP データベースに登録されているアクセスポイントに新規のプロファイルを適用した後は、アクセスポイントを再起動する必要があります。

「Administration」フォルダの「Basic Setup」ページの各種タブを使用して行った設定は、すべてデフォルト AP プロファイルの設定となります。これらの設定に変更を加えると、このデフォルトプロファイルを使用しているすべてのアクセスポイントに影響を与えます。

デフォルトプロファイルで設定するすべての項目は、お客様が作成する他のプロファイルでも使用することができます。新規プロファイルの設定方法およびアクセスポイントへの適用方法については、108 ページの「8.1 アクセスポイントプロファイルの作成、設定、管理」を参照してください。

ネットワーク

一般的に無線クライアントは、利用可能な無線ネットワークのリストから、ネットワーク（SSID で識別）を選択することによりアクセスポイントに接続を行います。SSID の登録を含むこれらの無線ネットワークの設定は、D-Link 統合スイッチにて行います。

WLAN 上で利用可能なネットワークの管理は、SSID、VLAN ID、セキュリティおよびトンネリングパラメータを含むネットワーク設定の変更または追加により行います。アクセスポイント設定プロファイルを使用して、仮想アクセスポイントによるネットワーク接続が可能です。

初期値では、スイッチは 8 つのネットワークに接続し、各ネットワークは各無線インタフェースに存在する 8 つの VAP のうちの 1 つと接続します。デフォルトネットワーク設定を変更して（但し削除はできません）新しいネットワーク設定を作成できます。1 番目のネットワークはデフォルト SSID「Guest Network」として設定します。他のネットワークにはネットワーク ID ベースで割り当てたデフォルト SSID を持たせます。すべてのデフォルトネットワークはオープン認証となっており、デフォルト VLAN 1 に割り当てられます。デフォルト VLAN は、ネットワークに RADIUS ベースの認証設定がない場合、または RADIUS サーバが特定のクライアントに VLAN 番号を返さない時などに使用されます。

ローカルアクセスポイント・データベース

統合スイッチがアクセスポイントを管理するために、Valid AP データベースにアクセスポイントの物理 MAC アドレスを登録する必要があります。Valid AP データベースはスイッチに、または外部の RADIUS サーバに保持できます。

アクセスポイントが検出されると、アクセスポイント側で「Managed Mode」が有効となり、認証済みの場合だけ、（必要時のみ）認証スイッチは認証モード（ローカルまたは RADIUS）に従ってアクセスポイントの MAC アドレスを認証します。アクセスポイントに妥当性が認められるとスイッチの管理下に入ります。

アクセスポイントが検出されても、その MAC アドレスが Valid AP データベース内に存在しない場合、またはアクセスポイントが認証に失敗した場合、スイッチはそのエントリを「AP Failure」リストに追加します。ローカル Valid AP データベースを使用している場合、認証に失敗したアクセスポイントを、「Authentication Failed Access Points」画面から Valid AP データベースに直接加えることができます。

Valid AP データベースには、アクセスポイントとその MAC アドレスの他に、AP モードやローカル認証パスワード、またアクセスポイントが使用している AP プロファイルなどの追加情報があります。また、各アクセスポイントに対し、手動でチャンネルや RF 信号送信電力などを設定でき、それらは AP プロファイル内の各項目より優先されます。

5.2 AAA と RADIUS の設定

D-Link 統合アクセスシステムでは、RADIUS サーバに以下の機能を持たせることができます。

- アクセスポイントに対するクライアント認証およびアカウンティングの管理
- スイッチに対するアクセスポイント認証およびアカウンティングの管理
- アクセスポイント設定用データベース

ここでは、アクセスポイントに対するクライアント認証およびアカウンティング管理に関する情報について説明します。スイッチに対するアクセスポイント認証については 51 ページの「アクセスポイント認証に RADIUS データベースを使用する」を参照してください。RADIUS サーバにアクセスポイントデータベースを設定する方法については 141 ページの「付録 B 外部 RADIUS サーバの設定」を参照してください。

WLAN > Administration > Basic Setup の「AAA/RADIUS」タブを選択して行う RADIUS サーバ設定は、デフォルト AP プロファイル用の RADIUS サーバのためのものです。各ネットワーク用の固有の RADIUS サーバ設定、またはデフォルト RADIUS サーバの使用が可能です。

AP に接続するのにクライアントが WPA エンタープライズ、または WEP IEEE802.1X セキュリティを使用する場合など無線クライアントと AP の通信のために RADIUS サーバを使用する場合、AP は、RADIUS クライアントとなり、RADIUS サーバと通信します。統合スイッチは AP と RADIUS サーバの間にパケットをトンネルします。これは、AP を RAIDUS サーバにおけるクライアントとして設定しなければならないことを意味します。RADIUS クライアントを設定する方法については 141 ページの「付録 B」を参照してください。

表 5-1 では、デフォルト AP プロファイル RADIUS サーバ設定用の各項目の内容を説明します。

表 5-1　グローバル RADIUS サーバ

設定項目	説明
IP Address	スイッチが認証に使用する RADIUS サーバの IP アドレス。
Secret	RADIUS サーバ用の秘密鍵。「Edit」チェックボックスにチェックを入れて、キーを入力します。入力時に周囲からキーを見られないように、入力した英数字は「*」で表示されます。
Accounting	システム時間、送受信したデータ量など、ユーザのリソース使用状況を記録します。

注意 「AP Profile」ページから RADIUS および MAC 認証設定情報に接続すると、プロファイル名欄が表示されます。プロファイル名を変更するためには、既存のプロファイル名を削除し、欄内に新規プロファイル名を入力し、「Submit」ボタンをクリックします。

「AAA/RADIUS」タブを使用し、アクセスポイントへのアクセスを許可 / 拒否する無線クライアントの MAC アドレスが記載されたグローバルリストを設定することができます。グローバルリストは、ローカル MAC 認証（SSID データ）を使用するプロファイルに対してのみ適用されます。MAC 認証は初期値では無効です。MAC 認証を有効にする方法については、62 ページの「デフォルトネットワークの設定」を参照してください。

「Default Action」として「Allow」（許可）を指定すると、「Allow MAC List」に登録された無線クライアントはアクセスポイントに接続でき、他のすべてのクライアントは接続を拒否されます。反対に、「Default Action」に「Deny」（拒否）を指定すると、「Deny MAC List」に登録されている無線クライアントは、アクセスポイントに接続できなくなります。

注意 MAC リストの表示は、選択された「Default Action」によって切り替わります。

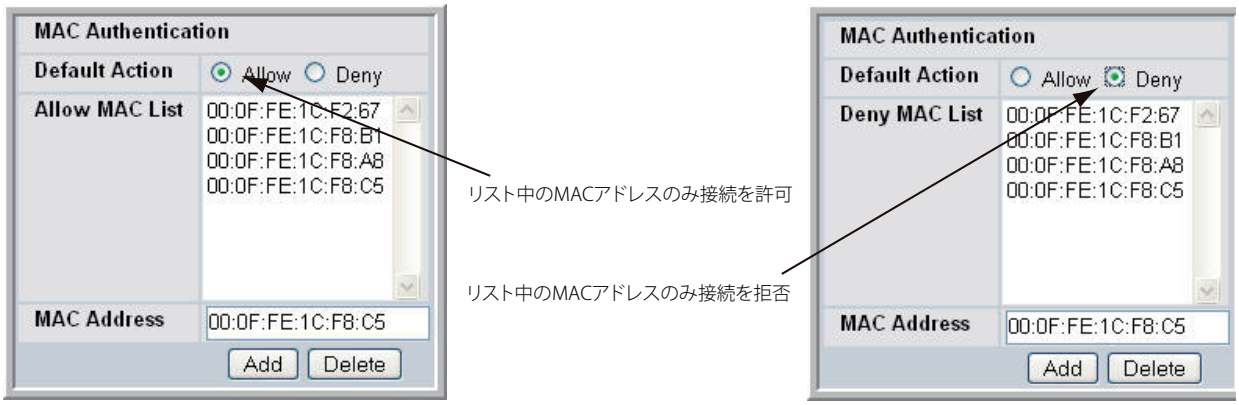


図 5-1　MAC アクセス制御

「MAC Authentication」リストに無線クライアントを追加するためには、「MAC Address」欄にクライアントの MAC アドレスを入力して、「Add」ボタンをクリックします。登録を有効にするためには「Submit」ボタンをクリックする必要があります。

以下に「MAC Authentication」リスト中の各項目の詳細を示します。

表 5-2　MAC 認証

設定項目	説明
Default Action	アクセスポイントに接続を試みる無線クライアントの取り扱いを指定します。 • Allow - 本リストに登録された MAC アドレスを持つクライアントだけに MAC 認証を使用するアクセスポイントとの接続を許可します。 • Deny - 本リストに登録された MAC アドレスを持つクライアントだけに MAC 認証を使用するアクセスポイントとの接続を拒否します。
MAC List	アクセスポイントへの接続許可 / 拒否の対象となるクライアントを表示します。
MAC Address	本プロファイルを使用するアクセスポイントへの接続を許可 / 拒否するクライアントの MAC アドレスを入力します。

5.3 無線電波の設定

DWL-3500AP は、1 つの無線インタフェース（IEEE 802.11g モード）をサポートしています。一方、DWL-8500AP は 2 つの無線インタフェース（IEEE 802.11a モードで運用する Radio 1 と IEEE 802.11g モードで運用する Radio 2）をサポートしています。

各モードの違いは、運用される周波数帯の違いです。IEEE 802.11g は 2.4GHz 帯を使用し、IEEE 802.11a は 5GHz 帯を使用します。
デフォルト無線設定は、**WLAN タブ > Administration > Basic Setup** から図 5-2 に示す「Radio」タブを使用して行います。

注意 IEEE 802.11g 用無線設定は、IEEE 802.11a 用と同じページの下段で行います。同じプロファイルを DWL-3500AP に適用する場合は、IEEE 802.11g 用の設定が適用されます。

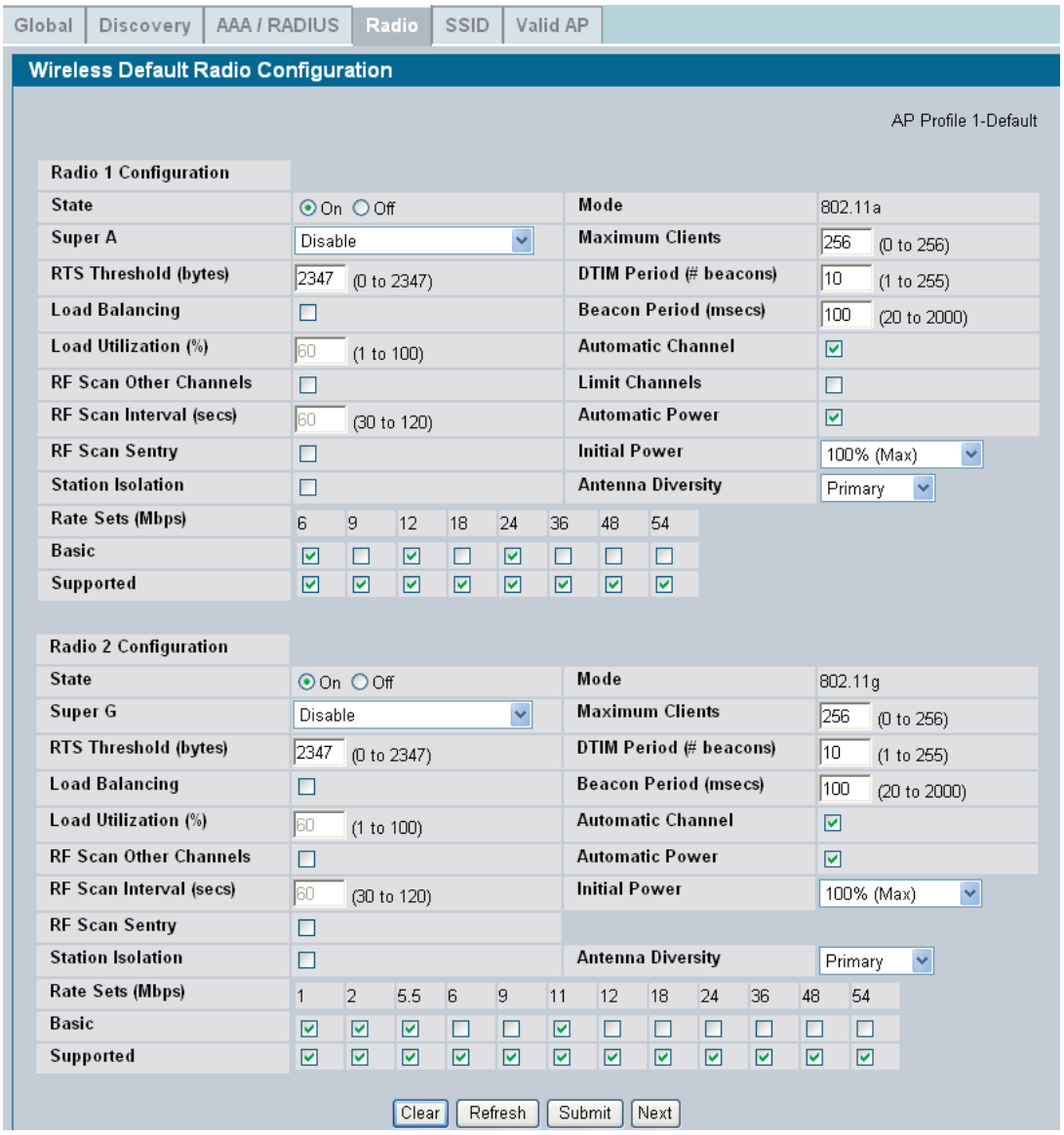


図 5-2　無線設定

以下の表は、「Basic Setup」画面の「Radio」タブを使用して無線設定をする際の各設定項目について説明しています。設定内容を変更した後は、「Submit」ボタンをクリックして設定を適用してください。

設定項目	説明
State	「On」または「Off」ラジオボタンを選択して、無線インタフェースをオンまたはオフにします。 無線インタフェースをオフにすると、アクセスポイントは配下のすべての無線クライアントに向けて接続解除フレームを送信します。この手順で無線インタフェースのシャットダウンが行われ、クライアントは他のアクセスポイントとの間で接続プロセスを開始します。
Super A Super G	Super A と Super G はバースト転送やフレーム圧縮により、パフォーマンスを改善する技術です。アクセスポイントが Super A と Super G 機能対応のクライアントと通信する場合にパフォーマンスが向上します。ただし、Super A または Super G 機能が有効な場合、アクセスポイントが消費する帯域は増加します。 • Super A または Super G 機能を有効にするためには「Enable」を選択します。 • Super A または Super G 機能を無効にするためには「Disable」を選択します。 • Super A または Super G 機能にダイナミック Turbo 機能を追加するためには「Enable with Dynamic Turbo」を選択します。

設定項目	説明
RTS Threshold (bytes)	RTS（送信要求）時のパケットサイズを指定します。この値を指定すると、特に多数のクライアントを抱えるアクセスポイントを通過するトラフィックフローの制御に役立ちます。 低い値を指定すると、RTS パケットは頻繁に送信されるようになります。これにより消費する帯域幅は増大し、パケットのスループットは低下します。一方、RTS パケットの送信数を増やす、混雑したネットワーク内で起こり得る干渉や衝突からの回避や、電磁波による干渉を軽減できるようになります。0 から 2347 の範囲で指定します。
Load Balancing	ロードバランシング機能を有効にすると、アクセスポイントにかかるトラフィック量を制御することができます。
Load Utilization (%)	その無線インタフェースでのネットワーク帯域使用率（%）のしきい値を設定します。このしきい値に使用率が達すると、アクセスポイントは新しいクライアントとの接続を拒否します。ここに 0 を指定すると、使用率にはかかわらず、すべての接続を許可します。
RF Scan Other Channels	アクセスポイントは RF スキャンを実行し、自分の通信範囲内の他の無線デバイスの情報を集め、統合スイッチに報告します。チェックボックスを選択すると、定期的に他のチャンネルのスキャンも行います。これにより、ユーザトラフィックの遮断が発生し、特に音声通信中はそれが顕著になります。チャンネルの変更をすると、自動キャリブレーション設定が失われ、信号品質が低下する場合があります。 チェックボックスのチェックを外すと、アクセスポイントは運用中のチャンネルのみスキャンします。
RF Scan Interval (secs)	RF スキャン中のアクセスポイントがチャンネルを変更する間隔を指定します。
RF Scan Sentry	チェックボックスを選択すると、RF スキャンを専門に実行します。無線インタフェースは送信されてくるビーコンフレーム、およびクライアントと他のアクセスポイント間のトラフィックを受動的に学習していますが、クライアントからの接続には応じません。Sentry（監視）モードでは、すべての VAP は無効になります。 本モードでは、スキャンはチャンネル間を移動して行われます。各チャンネルに費やす時間は「RF Scan Duration（スキャン時間）」によって制御されます。初期値は 10 ミリ秒です。
RF Scan Sentry Channels	無線インタフェースは 802.11b/g 周波数帯と 802.11a 周波数帯内のチャンネルのスキャンを行います。スキャンの対象となる周波数帯を選択します。 **注意** 周波数帯の選択は、「RF Scan Sentry」選択時のみ指定します。
Station Isolation	チェックボックスを使用し、station isolation を有効または無効にします。 • Enabled - アクセスポイントは無線クライアントの通信を防御します。アクセスポイントは、無線クライアントの中だけでなくネットワークの無線クライアントと有線デバイス間のデータトラフィックを許可します。 • Disabled - 無線クライアントは、通常通りアクセスポイントを経由してトラフィックを送信することでお互いに通信できます。 **注意** station isolation は、トンネルされないトラフィックを送信するクライアントにだけ操作が可能です。クライアントのトラフィックがトンネルされる場合、station isolation は、これを有効にしても、それらのクライアントには効果はありません。 **注意** station isolation は各帯域に個別に設定されます。SSID ごと、または AP ごとに station isolation を設定することはできません。
Rate Sets (Mbps)	アクセスポイントがサポートする通信速度（Transmission rate set）、およびアクセスポイントが通知をする速度（Basic rate set）を指定します。単位は Mbit/ 秒です。
Basic	ネットワーク内の他のアクセスポイントやクライアントとの通信を開始するために、アクセスポイントがネットワークに通知する通信速度です。一般的に、アクセスポイントがサポートする通信速度をブロードキャストするのが効率的です。
Supported	アクセスポイントがサポートする通信速度です。複数の速度を選択することができます。（チェックボックスをクリックすることで、選択または非選択できます。）エラー率やアクセスポイントとクライアントとの距離などの要素をもとに、アクセスポイントは最も効率の良い速度を自動的に選択します。
Mode	無線インタフェースが使用する物理層（PHY）の標準を定義します。 • DWL-3500AP および DWL-8500AP の Radio 1 は IEEE 802.11g モードの物理層標準を使用します。このモードは 802.11b と同じ 2.4GHz 帯を利用していますが、802.11b より高速化されています（最大通信速度 54Mbps）。直交周波数分割多重（OFDM）方式を採用し、1~54Mbps の通信速度をサポートします。また IEEE 802.11b と互換性があり、IEEE 802.11b 対応のクライアントも 802.11g モードを使用できます。 • DWL-8500AP の Radio 2 は IEEE 802.11a モードの物理層標準を使用します。5GHz 内の U-NII 帯域を利用し、OFDM 方式を採用しています。また 6~54Mbps の通信速度をサポートします。 無線インタフェースが無効に設定の場合、本モードは「Off」と表示されます。
Maximum Clients	最大クライアント数。本アクセスポイントに一度にアクセスできるクライアントの数を指定します。（0~256）
DTIM Period (#beacons)	DTIM 間隔。DTIM メッセージはビーコンフレームに含まれる要素です。DTIM は省電力モード中の無線クライアント向けのデータがアクセスポイントに送信待ちとしてバッファされていることを示しています。 ここで指定する DTIM Period（DTIM 間隔）は、本アクセスポイントの配下にあるクライアントが、アクセスポイントにバッファされているデータを確認する間隔を示します。1 ～ 255 の範囲で指定します。 数字はビーコンの数で表します。例えば、ここに「1」と入力した場合、バッファされたデータの確認は、ビーコンフレーム送信ごとに行われます。「10」と入力した場合は 10 回のビーコンフレーム送信に 1 度の確認となります。

設定項目	説明
Beacon Period (msecs)	ビーコン間隔。ビーコンフレームは無線ネットワークの存在を通知するために、アクセスポイントから定期的に送信されます。初期状態では、ビーコンフレームは 100 ミリ秒に 1 度（1 秒に 10 回）送信されます。 単位はミリ秒です。20 ～ 2000 の範囲から指定します。
Automatic Channel	チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。チャンネルの範囲および初期設定のチャンネルは、無線インタフェースのモードにより決定されます。 アクセスポイントが再起動する時、アクセスポイントは RF エリア内で使用されているチャンネルをスキャンし、干渉のない空きチャンネルを選択します。 ただし、チャンネルの状況は刻々と変化しています。 「Automatic Channel」を有効にすると、本プロファイルを適用したアクセスポイントでは、自動チャンネル選択が可能になります。自動的に、または手動で自動チャンネル選択アルゴリズムを実行させ、WLAN 状態の変化に伴って統合スイッチに AP が使用するチャンネルの調整をするようにすることができます。 初期値では、グローバル自動チャンネルモードは「マニュアル」に設定されています。自動チャンネル選択モードを有効にする場合は「AP Management」から「RF Management」ページを開き、「Channel Plan Mode」に「Fixed time」または「Interval」を選択して実行タイミングを指定します。また、「Manual Channel Plan」ページで、手動で自動チャンネル選択アルゴリズムを実行させることも可能です。 **注意** 「Valid AP database」中で、または「Advanced AP Management」ページでアクセスポイントにスタティックチャンネルを割り当てている場合、そのアクセスポイントでは自動チャンネル選択を有効にできません。
Limit Channels	802.11a モードが指定されている場合、本チェックボックスを選択して、アクセスポイントが使用可能なチャンネルからチャンネル選択できるようにします。 **注意** 使用可能なチャンネルは、アクセスポイントを使用する国によって異なります。
Automatic Power	自動電力調整。送信電力レベルは、アクセスポイントがどれだけ遠くまで RF 信号をブロードキャストできるかということに関係します。電力レベルが低すぎると、無線クライアントが信号を検知できなかったり、WLAN のパフォーマンスが低下するということが起こります。逆に、電力レベルが高すぎると、RF 信号が通信範囲内の他のアクセスポイントとの間に干渉を起こす可能性が出てきます。 自動送信電力調整機能では、独自のアルゴリズムを使用して、RF 信号がなるべく遠くの無線クライアントまで到達し、かつ他のアクセスポイントがブロードキャストする RF 信号と干渉を起こすほど遠くまでは到達しないように、自動的に調整を行います。電力レベルアルゴリズムはパケット再送エラーの有無に基づき送信電力を 10%の割合で増減します。
Initial Power (%)	初期電力レベル。自動電力調整アルゴリズムは、ここで指定した送信電力の割合以下に電力を落とすことはありません。初期値の初期電力レベルは 100%になっています。つまり、自動電力調整を有効にした場合、RF 信号送信電力は増加することがあっても減少はしません。 単位は RF 信号の最大送信電力に対するパーセンテージ（%）です。
Antenna Diversity	無線のトラフィックを送受信するために使用するアンテナを選択します。 Auto - トラフィックを送受信するために最適なアンテナを自動的に選択します。最も良いアンテナを選択して、送って、受ける。 • Primary - トラフィックを送受信するためにプライマリアンテナを使用します。 • Secondary - トラフィックを送受信するためにセカンダリアンテナを使用します。

WLAN タブ > Administration > Advanced Configuration > AP Profiles をクリックし、「Default」タブをクリックします。次に「Radio」タブをクリックし、「Access Point Profile Radio Configuration」にアクセスすると、さらに詳細な設定をすることができます。

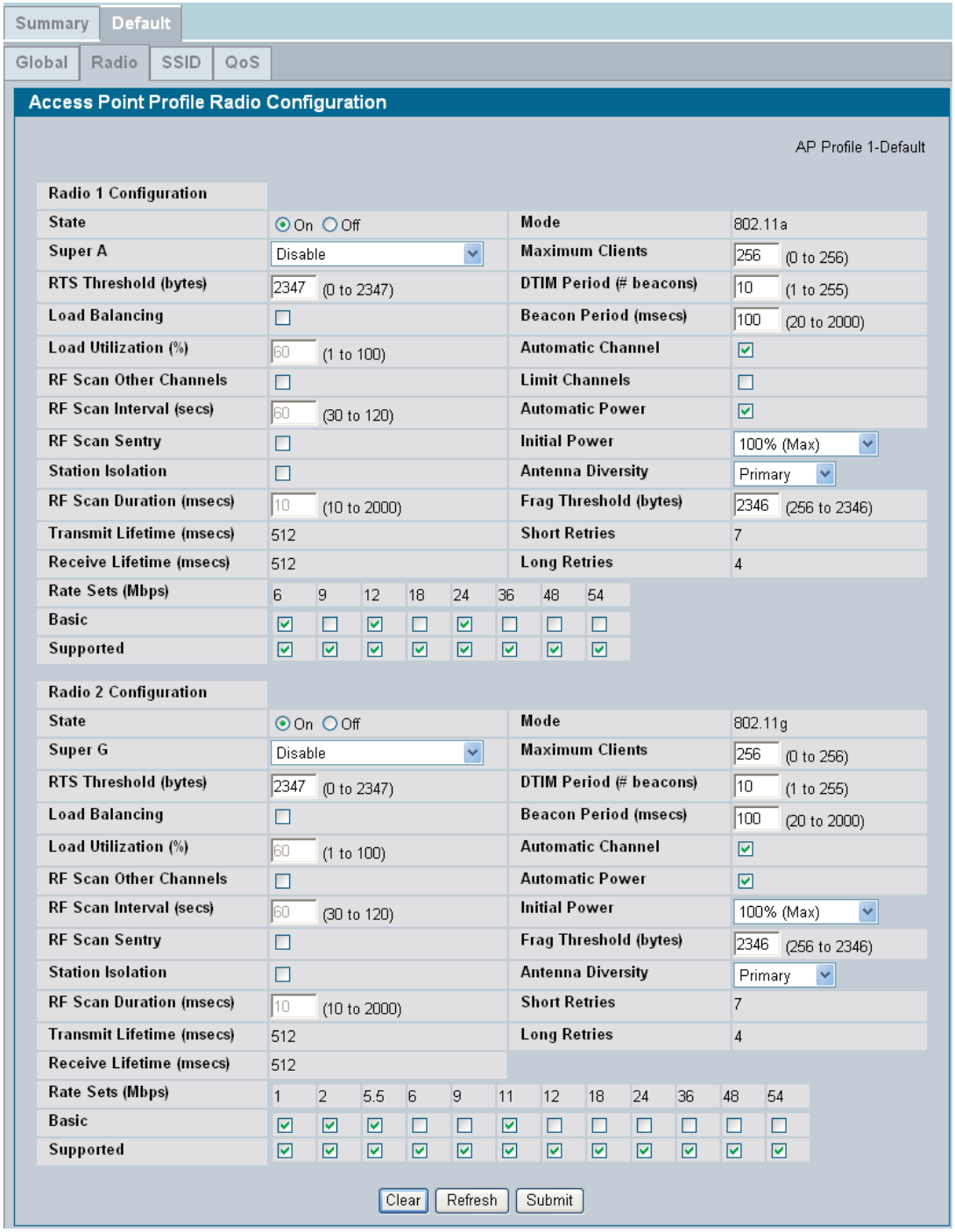


図 5-3　詳細無線設定

「Advanced Configuration」メニューで使用できるアクセスポイント無線関連項目について説明します。

設定項目	説明
RF Scan Duration (msecs)	RF スキャン時に他のチャンネルのスキャンに要する時間を指定します。単位はミリ秒です。
Transmit Lifetime (msecs)	最初の MSDU 送信から送信リトライを終了までの時間を指定します。単位はミリ秒です。
Receive Lifetime (msecs)	最初にフラグメント化された MMPDU または MSDU を受信してから、MMPDU または MSDU 再構築のリトライを終了するまでの時間を指定します。単位はミリ秒です。
Frag Threshold (bytes)	フラグメントしきい値。ネットワーク上で伝送されるパケットサイズを制限します。256 ～ 2345 の範囲で指定します。ここで指定したサイズ以下のパケットはフラグメント化されません。2346 という値は、パケットはフラグメント化されないことを示します。
Short Retries	RTS Threshold と同じ、またはそれより小さいサイズのフレーム送信の最大リトライ回数を示します。1 ～ 255 の範囲で指定します。
Long Retries	RTS Threshold より大きいサイズのフレーム送信の最大リトライ回数を示します。1 ～ 255 の範囲から指定します。

5.4 SSID の設定

SSID タブでは、デフォルト IP プロファイルに関連する仮想アクセスポイント（VAP）設定を示します。各 VAP に対し 1 つのネットワークが接続しており、ネットワーク番号や SSID により識別します。各物理アクセスポイントの無線インタフェースごとに 8 つまでの VAP を定義できます。
WLAN タブ > Administration > Advanced Configuration > AP Profiles の順にメニューをクリックし、プロファイルを選択後、「SSID」タブをクリックして以下の画面を表示します。

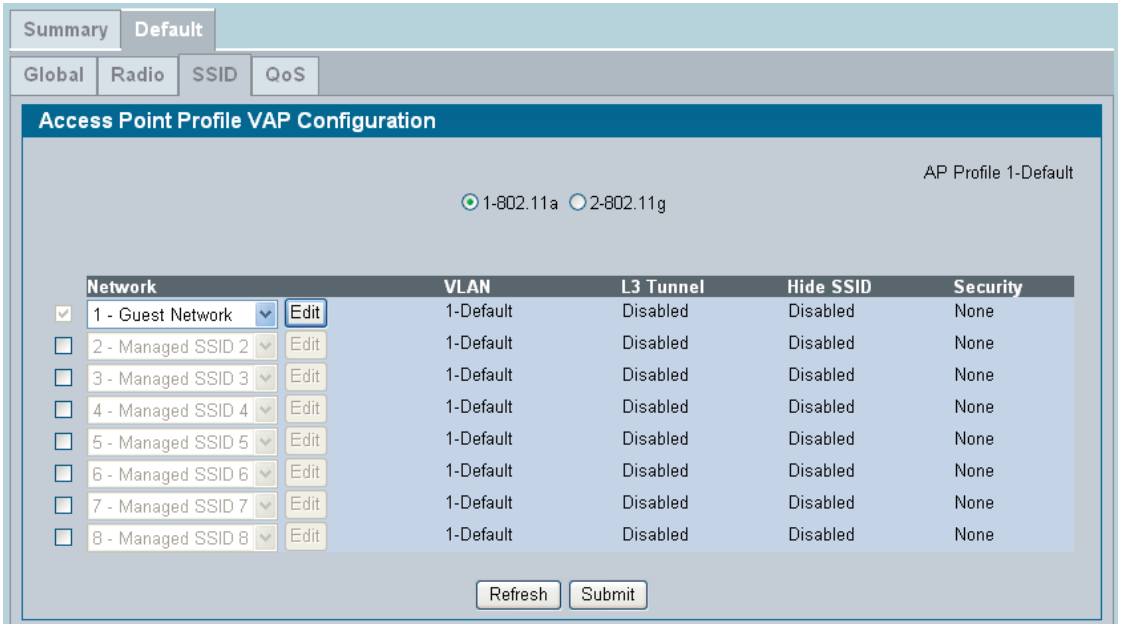


図 5-4　VAP 設定

イーサネットの VLAN と同様に、無線 LAN は VAP により複数のブロードキャストドメインに分割することができます。各無線クライアントにとって、各 VAP は 1 台の物理アクセスポイントと同じように見えます。しかし、それぞれの VAP は同じチャンネルを使用するため、1 台のアクセスポイント上のネットワーク間では RF 干渉が発生するリスクがありません。

VAP の使用により、ブロードキャストやマルチキャストのトラフィック管理が容易になり、ネットワークのパフォーマンスも向上します。また、VAP ごとに異なるセキュリティ方式を設定することも可能です。

VAP は「物理的な」エンティティ（存在）です。各 VAP は 1 つの MAC アドレスに対応します。一方、ネットワークは各 VAP に対して割り当てる「論理的な」エンティティです。ネットワークはネットワーク番号と SSID で認識します。SSID はネットワークごとに固有のものである必要はありません。1 つのネットワークの作成または変更を行い、それを 1 つまたはそれ以上の VAP に割り当てることができます。これにより、異なるプロファイルのネットワークを、すべての設定をやり直すことなく構成することができます。複数の VAP に割り当てたネットワーク設定を編集する場合は、そのネットワークを使用するすべての VAP に対して編集を行います。

仮想アクセスポイント設定の管理

デフォルト AP プロファイルでは初期値で 1 つの VAP が有効になっています。デフォルト VAP は SSID に「Guest-Network」を使用しており、無線クライアントからの VAP 接続を防ぐセキュリティを使用していません。他の VAP を有効にするためには、VAP の隣のチェックボックスにチェックを入れます。（図 5-4 参照）有効にした VAP にはプルダウンメニューからネットワーク（SSID）を選択することができます。ネットワーク設定内容を変更するためには「Edit」ボタンをクリックします。

以下の表に SSID 設定用ページの各項目の詳細を示します。

表 5-5　デフォルト VAP 設定

項目	説明
1-802.11a 2-802.11g	VAP の設定は 802.11a と 802.11g について別々に行います。VAP を有効にする前に、設定する無線インタフェースを選択します。
チェックボックス	指定した無線インタフェースの指定した VAP を有効または無効にします。チェックを入れると VAP は有効になります。チェックを入れることにより、同ページ内の SSID 欄において選択した VAP のネットワーク選択が可能になります。 **注意** デフォルト VAP および VAP 0 は無効にできません。
Network	VAP に割り当て可能なネットワークが表示されます。本スイッチには 64 個の異なるネットワークが登録可能で、それらを複数の無線インタフェースおよび VAP インタフェースに適用できます。初期値では 8 つのネットワークが登録済みで、各無線インタフェースの VAP に割り当てられています。 新規のネットワークを登録するためには「Advanced Configuration」から「Networks」をクリックしてください。
Edit	選択したネットワークの設定を変更する場合、本ボタンをクリックします。「Wireless Network Configuration」ページが表示されます。

項目	説明
VLAN	VAP の VLAN ID を表示します。設定内容を変更するためには、「Edit」ボタンをクリックします。
L3 Tunnel	VAP において L3 トンネリングが有効または無効であるかを表示します。設定内容を変更するためには、「Edit」ボタンをクリックします。 **注意** L3 トンネリングが有効である時、VLAN ID は使用されません。実際の運用ではスイッチはトンネリングするパケットに管理用 VLAN ID を記載しています。
Hide SSID	VAP が SSID のブロードキャストするかどうかを表示します。「Enabled」と表示されている時、そのネットワークの SSID は AP ビーコンフレームに含まれません。設定内容を変更するためには、「Edit」ボタンをクリックします。
Security	VAP の現在のセキュリティ設定を表示します。設定内容を変更するためには、「Edit」ボタンをクリックします。

デフォルトネットワークの設定

各ネットワークは SSID によって識別されます。SSID は英数字のキーで無線 LAN を識別します。D-Link 統合スイッチ上に 64 個のネットワークを設定することができます。各ネットワークに固有の SSID を、または複数のネットワークに同一の SSID を設定することも可能です。

VAP 設定用ページの「Edit」ボタンをクリックすると、図 5-5 で示すような無線ネットワーク設定用のページが開きます。

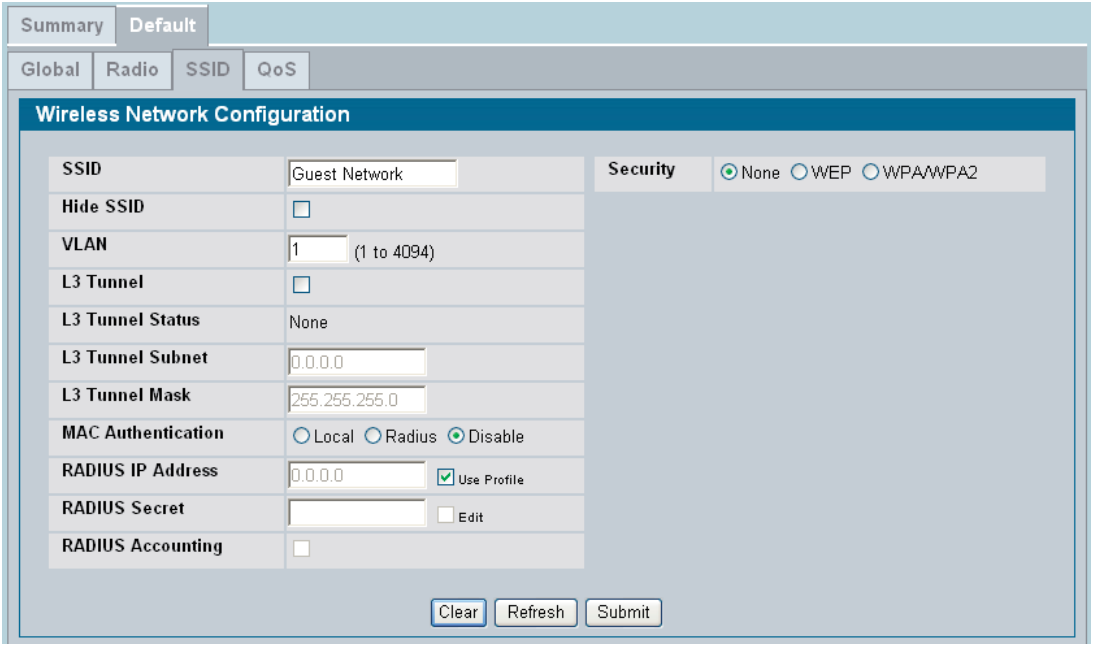


図 5-5　ネットワークの設定

以下の表では「Wireless Network Configuration」画面の各設定項目の詳細を説明します。無線ネットワーク設定の入力を終了後、「Submit」ボタンをクリックして設定を保存します。

設定項目	説明
SSID	無線クライアントは SSID によって無線ネットワークを識別します。SSID とは無線 LAN を一意に識別する半角英数字から成るキーです。SSID は 32 文字以内で指定し、使用する文字に制限はありません。
Hide SSID	SSID を非公表にします。SSID のブロードキャストを無効にすることにより、クライアントによるアクセスポイントの自動検出を阻止します。SSID を隠すと、クライアント側の「使用可能ネットワークリスト」にネットワーク名が表示されなくなります。その代わりに、クライアントは接続前に、サプリカントに接続する相手の正しいネットワーク名を登録する必要があります。SSID のブロードキャストを無効にすることで、あるクライアントが偶然ネットワークに入ってくることを防ぐことができます。しかし、ハッカーからの簡単な攻撃を防いだり、暗号化されていないトラフィックを監視するためには十分ではありません。本機能は、ゲストネットワークのような、クライアントからの接続が容易であることに重点を置いた、比較的無防備なネットワークに対して、最低限のレベルの防御を提供するものです。
VLAN	仮想 LAN は、ソフトウェアベースで 1 つのネットワーク上のデバイスを論理的にグループ分けしたもので、あたかも 1 つの物理ネットワークであるかのような動きをします。VLAN 内のノードはリソースや帯域を共有し、ネットワーク内で独立しています。D-Link 統合アクセスシステムは無線 VLAN をサポートしています。各 VAP を 1 つの VLAN 上に配置したり、他の VAP と同一の VLAN に所属させることもできます。 無線クライアントが SSID を使用してアクセスポイントに接続する場合、アクセスポイントはクライアントのトラフィックに、ここで入力した VLAN ID をタグ付けします。初期設定ではすべてのネットワークは VLAN 1 であり、初期値ではタグなしになっています。 **注意** ここに設定した VLAN ID は、RADIUS サーバ側に設定されているアクセスポイントの VLAN ID に上書きされます。つまり、ネットワークが無線クライアントを VLAN に割り当てるために RADIUS サーバを使用している場合、その無線クライアントは RADIUS サーバからの VLAN ID を使用し、VAP に設定されている VLAN ID は無視します。

設定項目	説明
L3 Tunnel	L3 トンネル機能。L3 トンネル機能では、モバイルステーションが 1 つのアクセスポイントから他のアクセスポイントにローミングする際に、これらのアクセスポイントが異なる IP サブネットに属している場合でも IP 接続を維持することができます。 **注意** L3 トンネルが有効である時、VLAN ID は使用されません。実際の運用ではスイッチはトンネリングするパケット上に管理用 VLAN ID を載せています。 **注意** L3 トンネリング機能が使用中に DWS-3000 スイッチが再起動するなど無線ネットワークトポロジが変更された場合、トンネルされているネットワークへの接続性を再確立する処理を直ちに行うために有線クライアントに対して ARP リフレッシュを実行する必要があります。 本機能を有効にする前に、ご使用のネットワークが 21 ページの「2.3 レイヤ 3 ローミング実現のためのネットワーク設計」の必要条件を満たしていることを確認してください。 L3 ローミングネットワークの詳細情報については、65 ページの「L3 トンネル用 VAP の設定」を参照してください。
L3 Tunnel Status	L3 トンネリングの状況を表示します。トンネリングの設定を正しくするためには、ルーティングを有効にし、スイッチにはトンネルサブネット内のルーティングインタフェース IP アドレスを持つ必要があります。トンネリング状況は、以下の 4 つのうちのいずれかになります。 • None（L3 トンネリング機能が無効になっています。またはネットワークに AP プロファイルが関連付けられていません。） • Configured（設定済み） • Not Configured-Routing Disabled（設定なし - ルーティング無効） • Not Configured-No Routing Interface（設定なし - ルーティングインタフェースなし）
L3 Tunnel Subnet	L3 トンネルサブネット。ここに入力するネットワーク IP アドレスは、スイッチに定義した WLAN 用ルーティングインタフェースと同一サブネット内で指定します。
L3 Tunnel Mask	L3 トンネルマスク。L3 トンネルサブネット上のネットワーク IP アドレス用サブネットマスクを入力します。
MAC Authentication	MAC 認証。MAC 認証を有効にしている時、無線クライアントがネットワークに接続するために、アクセスポイントにより認証を受ける必要があります。クライアントの MAC アドレスを以下のいずれかのデータベースに登録し、（AP プロファイルに設定したアクションに基づき）接続の許可または拒否を行います。 • ローカル • RADIUS
RADIUS IP Address	RADIUS サーバの IP アドレス。無線クライアントの認証に RADIUS サーバを使用している場合は、プロファイル用に「AAA/RADIUS」タブ上で設定したものと同じ RADIUS サーバを使用できます。また、他の RADIUS サーバを指定することも可能です。本 VAP 用に RADIUS サーバを指定するためには、「Use Profile」チェックボックスのチェックを外し、ここに RADIUS サーバの IP アドレスを入力してください。
RADIUS Secret	RADIUS サーバの秘密鍵。秘密鍵を登録するためには、「Edit」チェックボックスにチェックを入れてここに秘密鍵を入力します。
RADIUS Accounting	RADIUS アカウンティング機能。本チェックボックスにチェックを入れると、指定した RADIUS サーバに登録した無線クライアントのアカウンティングを有効にします。
Security	デフォルト AP プロファイルには、初期状態ではセキュリティが使用されていません。ネットワークを保護するために、セキュリティ方式を指定し、権限のないクライアントのネットワーク侵入を防ぐことを強くお勧めします。 以下の WLAN ネットワークセキュリティオプションが選択できます。 • None（セキュリティなし） • WEP • WPA/WPA2 セキュリティ方式として WEP または WPA/WPA2 を選択すると、ダイアログボックスが表示されネットワークセキュリティの変更を確認します。「OK」ボタンをクリックすると、新しい欄が表示され、変更したネットワーク設定内容はスイッチに反映されます。 各セキュリティ方式および追加項目の詳細については、66 ページの「アクセスポイントのセキュリティ設定」を参照してください。

D-Link のアダプタブルな無線技術は、無線ネットワーク（SSID）と VLAN またはトンネルサブネットを関連付けるための選択を提供します。SSID と VLAN を関連付けるために、「VLAN」欄に VLAN ID を入力します。SSID とトンネルサブネットを関連付けるために、「L3 Tunnel」を有効にし、「L3 Tunnel Subnet」と「L3 Tunnel Mask」欄を入力します。

D-Link のアダプタブルな無線技術は、柔軟性を最大にします。無線アプリケーションは、トラフィックが扱われる方法を決定します。例えば、ゲストトラフィックはセキュリティコントロールを集中管理のためにスイッチにトンネルされ、VoIP トラフィックは最適な性能のために VLAN ID でタグ付けされ、アクセスポイントから直接送信されます。

新規 VAP の設定および有効化

無線クライアントが利用可能な無線ネットワークを検索する場合、クライアントからは、「VAP」タブ上で有効にした VAP がそれぞれ別のネットワークのように見えます。図 5-6 は 5 つの VAP が有効である AP プロファイルの例を示します。各 VAP は異なるネットワークを使用しています。

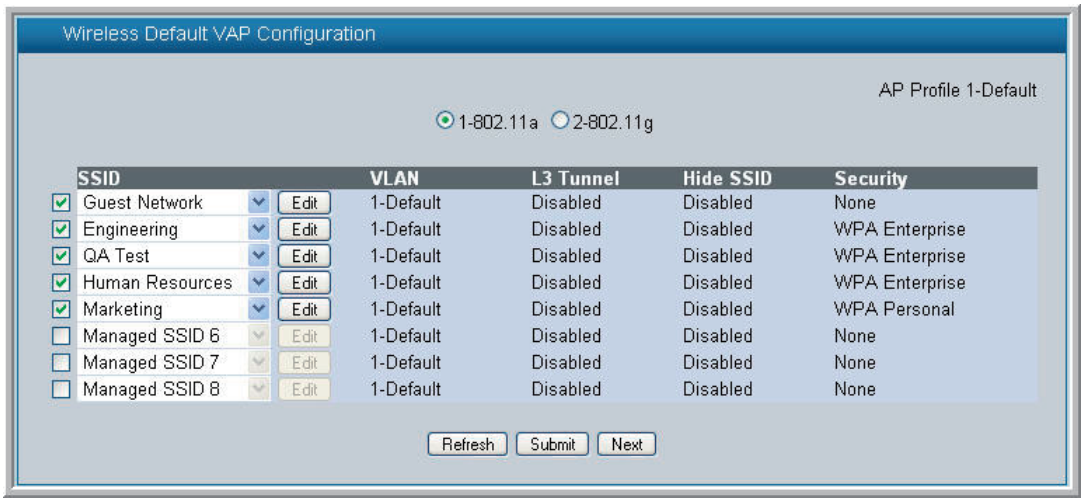


図 5-6　5 つの有効 VAP を持つ AP プロファイル

図 5-7 では、ユーザが通信範囲内の無線ネットワークを検索する際の、Microsoft Windows XP クライアントの画面表示例を示しています。

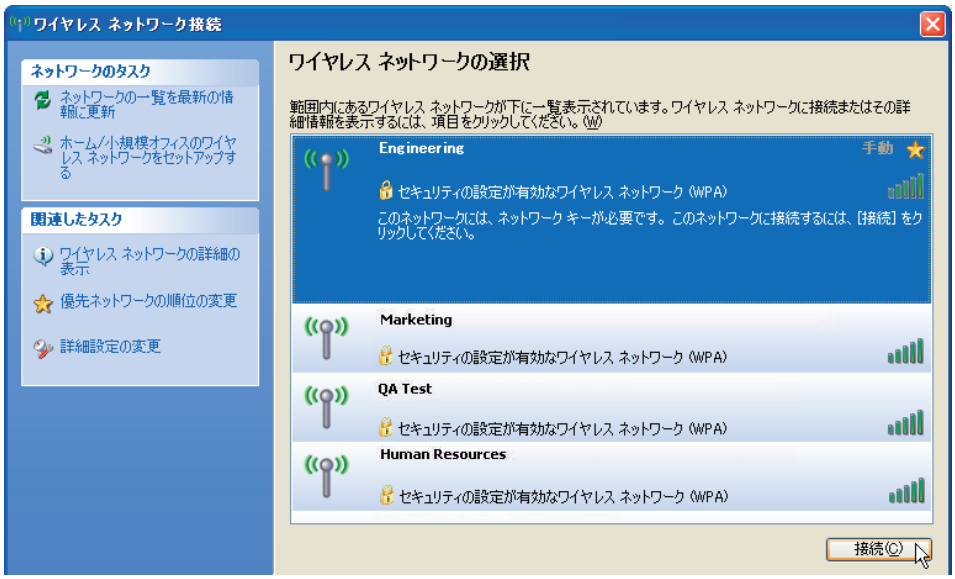


図 5-7　無線クライアントから利用が可能なネットワーク

ここでは無線クライアントは 4 つの異なる無線ネットワークを検出していますが、実際はすべて 1 台のアクセスポイント上に存在しています。D-Link アクセスポイントは無線クライアントから見ると、4 台の異なるアクセスポイントのように見えています。

この例では、管理者は会社内のグループ別に複数の VAP を作成しています。各 VAP に対しそれぞれ異なる SSID、セキュリティ設定、VLAN ID を与え、トラフィックを分割しています。

同一のネットワーク（SSID）を複数の VAP に割り当てることも可能です。この時クライアントからは、これらの VAP は 1 つのネットワークのように見えます。2 つの無線インタフェースの VAP に対して同一の設定を行うため、無線アダプタが 802.11a または 802.11b/g のどちらをサポートしていても、無線クライアントは同じネットワークに接続することができます。

初期状態では、どちらの無線インタフェースにも VAP に割り当てられた同じネットワークが存在し、VAP 0 のみが有効になっています。VAP の設定は無線インタフェースごとに行う必要があります。つまり、片方の無線インタフェースである VAP を有効にしても、もう一方の無線インタフェースの VAP は影響を受けることはありません。

L3 トンネル用 VAP の設定

本項では L3 トンネリング機能の概要を示します。L3 ローミングを使用するネットワークの詳細な設定例については、146 ページの「付録 C L3 ローミング設定例」を参照してください。

L3 トンネル機能を使用すると、無線クライアントが 1 つのアクセスポイントから他のアクセスポイントにローミングする際に、これらのアクセスポイントが異なる IP サブネットに属している場合でも IP 接続を維持することができます。

本機能は複数のサブネットに分かれた 802.11 ネットワーク上で、無線 VoIP（Voice over IP）を利用するような環境で特に有効な手段となります。

L3 トンネリングを有効にする場合は、本機能の利用が必要なクライアント用に別の VAP を設定し、有効にすることをお勧めします。L3 トンネリング機能を必要とするクライアントのみを L3 トンネリングが有効な SSID に接続し、それ以外のクライアントは L3 トンネリング無効の VAP を使用するように設定を行ってください。

一般的に、ローミングしながら時間依存型のデータの送受信をするクライアントのみが本機能を活用することをお勧めします。図 5-8 は D-Link 統合スイッチが管理する 2 台のアクセスポイントが存在するネットワークを示しています。アクセスポイントとスイッチはそれぞれ異なるサブネットに属しています。

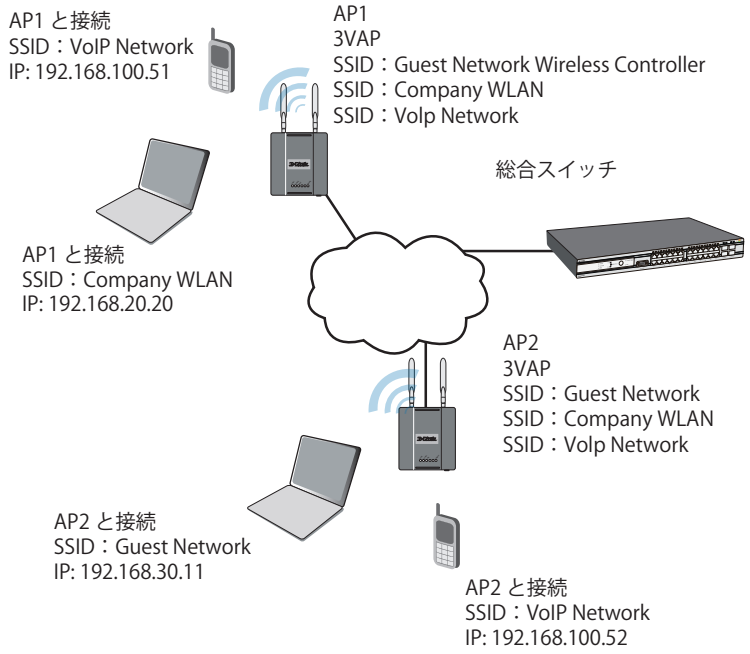


図 5-8　L3 ローミングの例

図 5-8 中の 2 台のアクセスポイントは両方とも同じデフォルトプロファイルを使用しています。デフォルトプロファイルでは 3 つの仮想アクセスポイント（VAP）が有効になっており、各 VAP は異なるネットワーク（SSID）を使用しています。ユーザが利用可能な無線ネットワークを検索する時、すべての SSID がネットワークリストに表示されます。ノート型 PC のクライアントは「Company WLAN」または「Guest Network」に接続し、VoIP 電話は「VoIP Network」に接続しています。

L3 トンネリング機能は「VoIP Network」で有効ですが、「Company WLAN」と「Guest Network」では無効になっています。これは、これら 2 つのネットワークではデータトラフィックが中心となっているためです。「VoIP Network」は音声トラフィック用のネットワークです。L3 ローミングは IP トンネリングを使用するので、アクセスポイントが異なるサブネットに存在していても、クライアントには同じサブネットのように見えています。

図 5-8 のサンプルネットワークが示すように、ノート型 PC のクライアントは 2 つの異なるアクセスポイントの異なる WLAN ネットワークに接続しています。インターネット電話ユーザは 2 つの異なるアクセスポイントの同じ WLAN ネットワークに接続しています。VoIP ネットワーク上では、インターネット電話ユーザはサービスの中断や再認証、ネットワークの変更などの必要もなく、AP1 と AP2 の間をシームレスにローミングすることができます。

統合スイッチは L3 トンネリングネットワーク用に設定された別の論理ネットワークとして、VLAN ルーティングインタフェースを使用します。このネットワークは L3 トンネリングサブネットでネットワークアドレス 192.168.100.0 を持ちます。

トンネリングがポートベースルーティングインタフェースと共には動作しません。トンネルされるすべてのルーティングインタフェースは VLAN ルーティングインタフェースである必要があります。また、同様に AP は、ポートベースルーティングインタフェース経由で関連付けされるべきではありません。

L3 トンネリング機能が使用中に DWS-3000 スイッチが再起動するなど無線ネットワークトポロジが変更された場合、トンネルされているネットワークへの接続性を再確立する処理を直ちに行うために有線クライアントに対して ARP リフレッシュを実行する必要があります。

CLI コマンドおよび Web インタフェースによる、L3 トンネリングを利用するためのネットワーク設定方法については、146 ページの「付録 C L3 ローミング設定例」を参照してください。

アクセスポイントのセキュリティ設定

デフォルト AP プロファイルには、初期状態でセキュリティが設定されていません。ネットワークを保護するために、セキュリティ方式を指定し、権限のないクライアントのネットワーク侵入を防ぐことを強くお勧めします。

WLAN タブ > Administration > Advanced Configuration > Networks の順にメニューをクリックします。

図 5-9 が示すように、「Wireless Network Configuration」ページで WLAN セキュリティ方式として「Security」を「None」、「WEP」、「WPA/WPA2」から 1 つ選択します。初期値では「None」が選択されています。

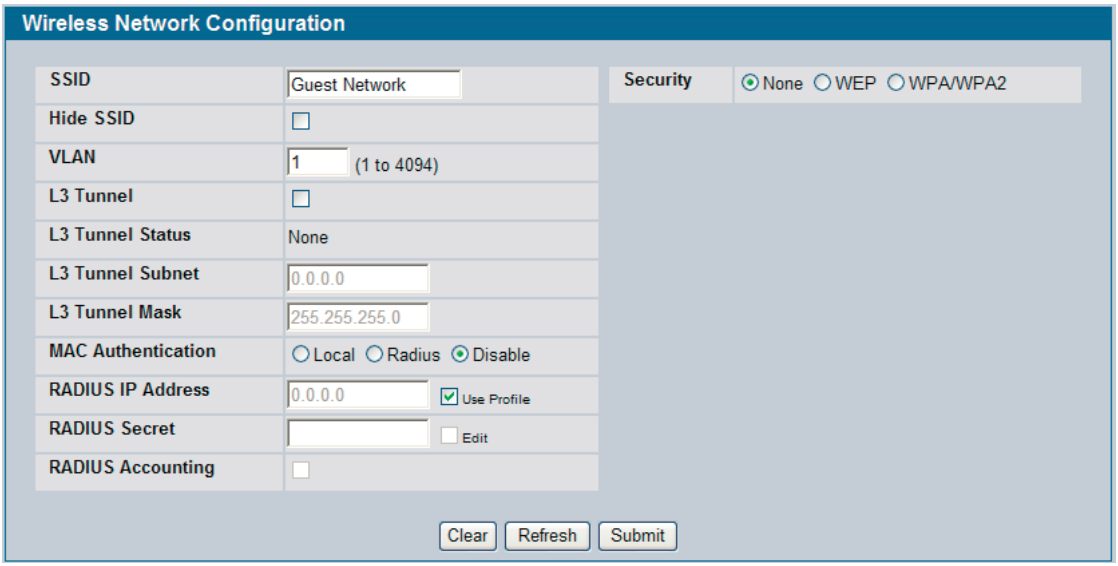


図 5-9　AP ネットワークセキュリティオプション

以下の項では、各セキュリティ方式について説明します。

セキュリティなし

セキュリティモードに「None」を選択すると、そのアクセスポイントに対してそれ以上の設定は不必要です。本モードでは、D-Link アクセスポイントと接続する無線クライアント間のデータ転送には暗号化が行われず、どんな無線クライアントでもアクセスポイントに接続が可能となります。

本セキュリティモードは初期のネットワーク設定時、または問題解決時の使用に便利です。しかし、本モードの選択は、安全性が極めて低いため、内部用ネットワークでの通常使用にはお勧めできません。

スタティック / ダイナミック WEP の使用

WEP（Wired Equivalent Privacy）は 802.11 無線ネットワーク用のデータ暗号化プロトコルです。本セキュリティ方式を選択すると、ネットワーク上のすべての無線クライアントやアクセスポイントは、データの暗号化に 64 ビット（秘密鍵 40 ビット + 初期化ベクタ（IV）24 ビット）、128 ビット（秘密鍵 104 ビット +IV 24 ビット）、または 152 ビット（秘密鍵 128 ビット +IV 24 ビット）の共有鍵を用います。

スタティック WEP は最も安全なモードではありませんが、外部ユーザが暗号化されてない無線トラフィックを探し出すのを防止することは可能であり、セキュリティモードに「None」を設定するよりもネットワーク保護に役立ちます。

ダイナミック WEP はスタティック WEP よりも安全性が高くなりますが、自動生成したキーの管理のために RADIUS サーバが必要となります。

WEP は無線ネットワーク中を移動するデータをスタティックキーを基に暗号化します（暗号化のアルゴリズムは RC4 と呼ばれるストリーム暗号です）。

セキュリティモードとして「WEP」を選択すると、図 5-10 に示すような新しい項目が表示されます。

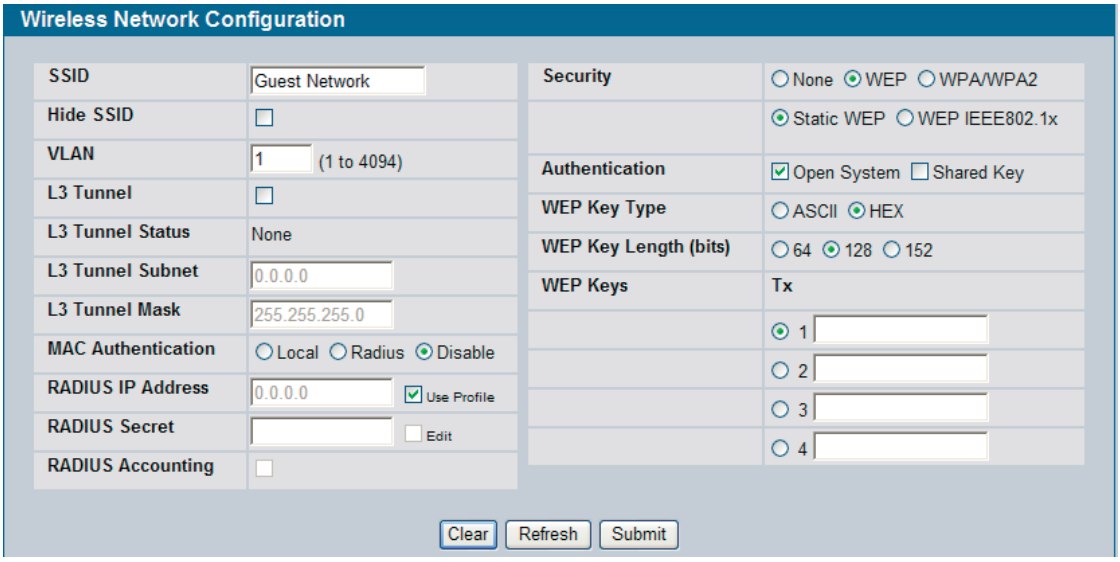


図 5-10　スタティック WEP の設定

表 5-8 に WEP 設定用オプションを示します。

表 5-8　スタティック WEP

項目	説明
Static WEP または WEP IEEE 802.1x	Static WEP（PSK）はスタティックキーを管理し使用します。無線クライアントとアクセスポイントの両方にデータを暗号化するための同じキーを手動で設定します。WEP IEEE 802.1x ではクライアントからアクセスポイントへのトラフィックの暗号化に動的に生成されたキーを使用します。WEP IEEE 802.1x は Static WEP より安全ですが、キーの管理のために RADIUS サーバが必要になります。EAP を選択すると、画面が更新されます。その他設定が必要な項目はありません。アクセスポイントはグローバル RADIUS サーバ IP アドレスと秘密鍵、または VAP に指定した RADIUS サーバの設定内容を使用します。統合スイッチにおいて、グローバル RADIUS サーバ設定の方法については、55 ページの「5.2 AAA と RADIUS の設定」を参照してください。
Authentication	認証タイプを選択します。 • Open System - 認証を行いません。 • Shared Key - 共通鍵。簡単なユーザ認証します。WEP キーをテキスト形式でクライアントに配布するため、オープンシステムより安全性が低いと考えられています。 • Both - WEP クライアントのみが認証されます。
WEP Key Type	ラジオボタンでいずれかのキータイプを選択します。 • ASCII - アルファベットの大文字、小文字、数字、および @ # などの記号。 • Hex - 16 進数。0~9 と A~F
WEP Key Length (bits)	ラジオボタンで 64 ビット、128 ビット、または 52 ビットの WEP キー長を選択します。
WEP Keys - Tx	送信キーインデックスは、アクセスポイントがどの WEP キーを送信するデータの暗号化に使用するかを示します。キー番号の左側にあるラジオボタンをクリックして送信キーを選択します。図 5-10 の例では、送信キー 1 を選択しています。
WEP Keys - 1 ～ 4	4 つまでの WEP キーを登録できます。各テキストボックスに、各キーの文字列を入力します。これらは RC4 WEP キーでアクセスポイントを使用するクライアントと共有します。 各キーには同じ文字数を使用します。登録するキーの文字数はキータイプとキー長によって異なります。入力するキーの文字数は以下の通りです。 • 64 ビット ASCII: 5 文字、Hex: 10 文字 • 128 ビット ASCII: 13 文字、Hex: 26 文字 • 152 ビット ASCII: 16 文字、Hex: 32 文字 各クライアントは、アクセスポイント用に指定したのと同じスロットに、同じ WEP キーから 1 つ登録します。

スタティック WEP 設定時のルール

スタティック WEP を使用する際は、以下のルールが適用されます。

- すべてのクライアントは WLAN セキュリティを「WEP」に設定し、アクセスポイントからクライアントへの送信データを復号するために、アクセスポイントで指定されている WEP キーのうちの 1 つを持つ必要があります。
- アクセスポイントは、クライアント側からのデータを復号するために、クライアントがアクセスポイントへの送信に使用するすべてのキーを持つ必要があります。
- すべてのノード（アクセスポイントとクライアント）で、キーは同じスロットを使用する。例えばアクセスポイントが「abc12」キーを WEP キー 3 と定義したならば、クライアント側も同じキーを WEP キー 3 と定義する必要があります。
- クライアントは、アクセスポイントへのデータ送信用にそれぞれ異なるキーを使用できます（複数のクライアントが同じキーを使用することもできますが、その場合は他のクライアントからのデータを解読できるため、安全性は低くなります）。
- 無線クライアントソフトウェアによっては、複数の WEP キーを登録し、「送信キーインデックス」を定義し、異なるキーを切り替えてデータを暗号化するように設定をすることもできます。これにより、近接するアクセスポイントがお互いの通信内容を解読できなくなります。
- アクセスポイントとクライアント間で、64 ビット、128 ビット、および 152 ビットの WEP キーを混在させることはできません。

WPA/WPA2 パーソナル / エンタープライズの使用

WPA と WPA2 は Wi-Fi Alliance により発表された IEEE 802.11i 標準に準拠した暗号化方式規格です。本規格は AES-CCMP および TKIP というメカニズムを採用しています。WPA/WPA2 パーソナルは事前共有キーを用いて証明書の初期チェックします。WPA/WPA2 エンタープライズでは RADIUS サーバを使用してユーザ認証します。

セキュリティモードとして「WPA/WPA2」を選択すると図 5-11 に示すような追加欄が表示されます。

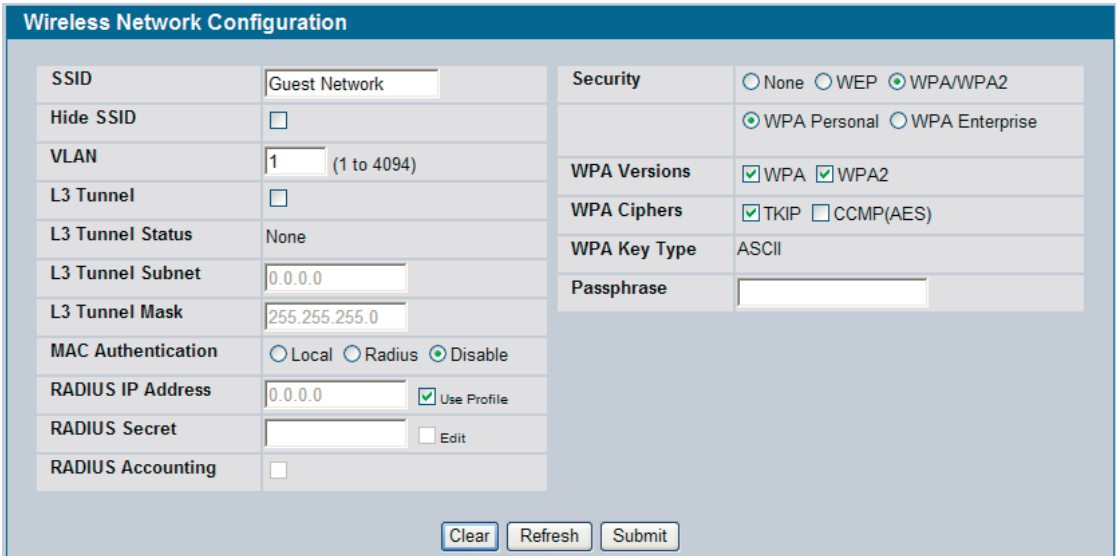


図 5-11　WPA パーソナルの設定

表 5-8 にスタティック WPA セキュリティモード用の設定オプションの内容を示します。

表 5-8　スタティック WPA

設定項目	説明
WPA Personal または WPA Enterprise	WPA/WPA2 パーソナルではスタティックキーを使用します。無線クライアント側とアクセスポイント側の両方に同じキーを設定し、データを暗号化します。 WPA/WPA2 エンタープライズでは RADIUS サーバを使用し、動的にキーを生成してクライアントからアクセスポイントへのトラフィックを暗号化します。WPA エンタープライズは WPA パーソナルより安全性が高いのですが、キーの管理のために RADIUS サーバを必要とします。 WPA エンタープライズを選択すると、画面が更新されて新しい設定用フィールドが表示されます（本表中で詳細を説明）。アクセスポイントはグローバル RADIUS サーバ IP アドレスと秘密鍵、または VAP に指定した RADIUS サーバの設定内容を使用します。AP は RADIUS クライアントとして機能して、RADIUS サーバにクライアントとして設定される必要があります。 統合スイッチにおいて、グローバル RADIUS サーバを設定する方法については、55 ページの「5.2 AAA と RADIUS の設定」を参照してください。
WPA Versions	サポートするクライアントステーションの WPA のタイプを選択します。 • WPA - ネットワーク上のすべてのクライアントが WPA をサポートし、WPA2 をサポートしていない場合は、WPA を選択します。 • WPA2 - ネットワーク上のすべてのクライアントが WPA2 をサポートしている場合は、IEEE 802.11i で最も安全なセキュリティを提供する WPA2 を使用することをお勧めします。 • WPA と WPA2 - WPA と WPA2 をサポートするクライアントが混在している場合は、両方のボックスを選択します。サポートする方式にかかわらずクライアント間の接続および認証が行えます。ただし、WPA2 サポートのクライアントに対しては、多少セキュリティは高くなります。本設定では相互運用性を実現する代わりに、セキュリティを若干低くしています。
WPA Ciphers	使用する暗号化方式を TKIP、CCMP(AES)、TKIP と CCMP(AES) から選択します。 TKIP と AES サポートのクライアントのどちらも、アクセスポイントへの接続が可能です。アクセスポイントとの接続のために、WPA クライアントは以下のどちらかを持っている必要があります。 • 有効な TKIP key • 有効な AES-CCMP key
WPA Key Type	ラジオボタンでどちらかのキー種別を選択します。 • ASCII - アルファベットの大文字、小文字、数字、および @ # などの記号。 • Hex - 16 進数。0~9 と A~F を使用。
Passphrase	パスフレーズ。WPA パーソナルで使用する WPA キーは共有秘密鍵です。8 から 63 の半角英数字を入力します。
Pre-Authentication	WPA/WAP2 エンタープライズを選択すると、事前認証が有効になります。 WAP2 対応の無線クライアントから事前認証パケットの送信をする場合は「Pre-Authentication」チェックボックスにチェックを入れます。事前認証情報はクライアントが接続中のアクセスポイントから、送信先のアクセスポイントに受け渡されます。本機能を有効にすると、ローミングするために複数のアクセスポイントと接続するクライアントの認証を高速化することができます。本機能は WPA2 を使用して接続するクライアントのみが利用できます。WPA ではサポートされていません。

設定項目	説明
Pre-Authentication Limit	アクセスポイントが同時に扱う事前認証数を入力します。このように制限することにより、RADIUS サーバへの過負荷を防ぐことができます。負荷が軽い状態では、事前認証パケットが再度送信されても拒否されません。「0」は制限しないことを示しています。 注意 本項目は「Advanced Configuration」から「AP Profiles」または「Networks」ページからネットワークにアクセスした場合にのみ設定が可能です。
Key Forwarding	チェックボックスを選択すると、無線クライアントがローミングすることを想定して、接続中のアクセスポイントから他のアクセスポイントに対して PMK（Pairwise Master Key）を送信することができます。 注意 本項目は「Advanced Configuration」から「AP Profiles」または「Networks」ページからネットワークにアクセスした場合のみ設定が可能です。
Key Caching Hold Time	アクセスポイントが PMK を保持している時間を分単位で指定します。これは RADIUS サーバが生成し、アクセスポイントに送信する PMK に対する設定です。この時間の制限は RADIUS サーバがある特定のユーザ用として「Session-Timeout」にここで指定する値よりも大きな値を返してきた場合は、その値が優先されますのでご注意ください。 注意 本項目は「Advanced Configuration」から「AP Profiles」または「Networks」ページからネットワークにアクセスした場合のみ設定が可能です。

5.5 Valid アクセスポイントの設定

Valid アクセスポイントリストへの登録は、**WLAN タブ > Administration > Basic Setup** とクリックして表示できる「Valid AP」タブ（図 5-12 参照）を使用して行うことができます。または、**WLAN タブ > Monitoring > Access Point > Rogue/RF Scan Access Point** 画面から登録することもできます。

「Valid AP」タブでは、各アクセスポイントに対しチャンネルや RF 信号送信電力レベルを指定します。また AP モードやローカル認証パスワード、さらにアクセスポイントが使用するプロファイルを指定することもできます。

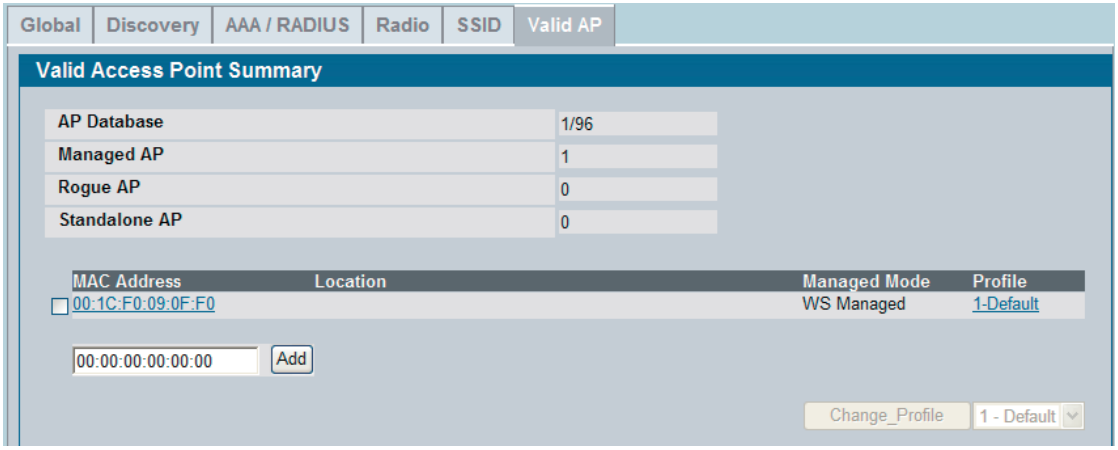


図 5-12　Valid アクセスポイントの登録

MAC アドレスとアクセスポイントの場所をリストに追加後、「Add」ボタンをクリックしてそのアクセスポイントをデータベースに追加し、そのアクセスポイント用の設定ページへ移行します。既にデータベース内に登録されているアクセスポイントについては、その MAC アドレスをクリックすると、それぞれの設定ページへ移行できます。

表 5-9 「Valid Access Point Summary」ページ

設定項目	説明
MAC Address	アクセスポイントの MAC アドレスを入力します。「Add」ボタンをクリックすると、そのアクセスポイントはスイッチのローカルデータベースに追加されます。
Managed Mode	現在のアクセスポイントの管理モードが表示されます。モードの設定は MAC アドレスをクリックしてアクセスできる「Valid Access Point Configuration」ページで行います。
Profile	アクセスポイントに適用されている AP プロファイルが表示されます。複数の AP プロファイルが登録されている場合は、本ページで他のプロファイルを適用することができます。該当するアクセスポイントのチェックボックス（複数選択可）にチェックを入れ、プルダウンメニューから適用するリストを選択します。「Change Profile」ボタンをクリックして変更を適用します。

アクセスポイント確認のためにローカルデータベースを選択すると、確認するアクセスポイントのデータベースはスイッチにより保持されます。データベースに MAC アドレスを追加すると、そのアクセスポイントは「WS Managed AP」または「Acknowledged Rogue」であるかを指定でき、またそのデバイスに適用する AP プロファイルを選択することができます。

スイッチが RF スキャンにより情報を収集すると、データベースにあるアクセスポイントに適切なステータスを割り当てます。

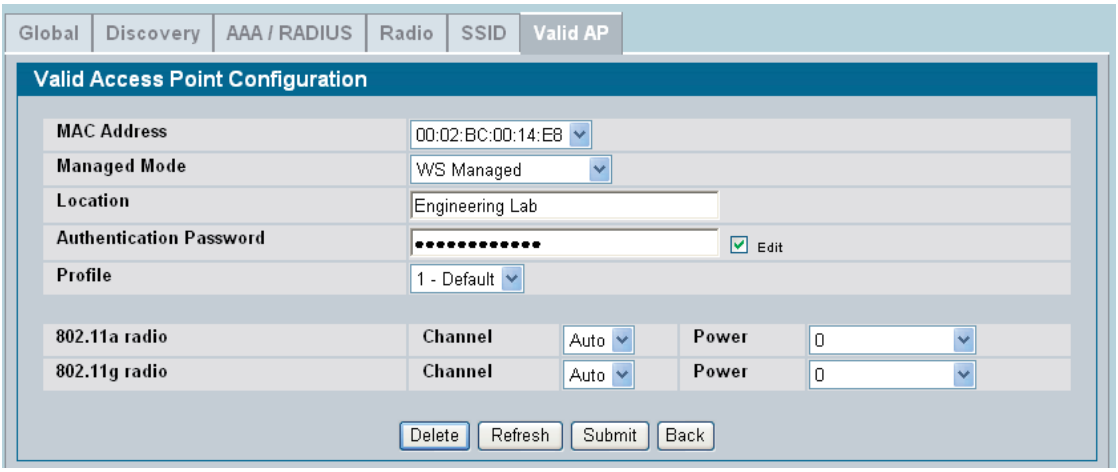


図 5-13　Valid アクセスポイントの設定

表 5-10 では「Valid Access Point Configuration」画面の各設定項目を説明します。

表 5-10 「Valid Access Point Configuration」画面

設定項目	説明
MAC Address	アクセスポイントの MAC アドレスが表示されます。この値を変更するためには、該当する Valid アクセスポイントの設定のすべてを削除し、MAC アドレスを登録し直す必要があります。
Managed Mode	D-Link アクセスポイントは以下の 3 種類の管理モードのいずれかに設定されます。 • Standalone - AP は、ネットワークにおいて個別のアクセスポイントとして機能します。スイッチを使用して AP を管理しません。代わりに、AP 自身のログインして、管理者用の Web ユーザインタフェース (UI) または CLI を使用することで管理します。 • WS Managed - D-Link アクセスポイントは D-Link 統合アクセスシステムの一部であり、D-Link 統合スイッチ（統合スイッチ）により管理されます。アクセスポイントが本モードの場合、管理用 Web インタフェースおよび SNMP サービスはアクセスポイントで使用できなくなります。 • Acknowledged Rogue - アクセスポイントがスイッチにより検出され不正であると認識されたものです。本アクセスポイントは D-Link アクセスポイントではありません。「Acknowledged Rogue（認識済みの不正）」の場合でも、悪意のあるアクセスポイントではないものとして、有効 AP リストに追加するが可能です。
Location	アクセスポイントを識別しやすくするために、場所を登録します。32 文字までの半角英数字を入力することができます。
Authentication Password	スイッチがアクセスポイントを検出する際にアクセスポイントの認証するように設定することができます。この設定は「Basic Setup」の下の「Global」タブで行いますが、パスワードはここで入力します。このパスワードはアクセスポイント上で登録されているものと一致する必要があります。
Profile	複数の AP プロファイルが登録されている場合は、プロファイルを選択してアクセスポイントに適用することができます。AP プロファイルの設定についての詳細は、108 ページの「8.1 アクセスポイントプロファイルの作成、設定、管理」を参照してください。
Channel	チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。チャンネルの範囲や初期設定のチャンネルは無線インタフェースのモードやアクセスポイントを使用する国により異なります。 日本の場合、IEEE 802.11b/802.11g モードではチャンネル 1 から 13 を使用し、IEEE 802.11a モードではより広範囲で非連続のチャンネル（36、40、44、48、52、56、60、64）を使用します。 複数のアクセスポイントが互いの範囲内において、同一または重複するチャンネル上でブロードキャストする時に干渉が発生します。大量のデータや中継トラフィックが帯域獲得のために争っているような高トラフィックの状況下では、干渉による影響は増大します。AP は、無線が再起動する時にはいつも最適なチャンネルを選択します。 「Auto」を選択すると、アクセスポイントは RF エリア内の既に占有されているチャンネルをスキャンし、干渉のない、または空いているチャンネルを自動的に選択します。 注意 チャンネルを指定する場合は、隣接するアクセスポイントが使用するチャンネルに干渉を与えないように注意してください。 注意 Valid AP データベース内のアクセスポイントに対して設定したチャンネルは固定され、アクセスポイントによる初期チャンネル選択や、スイッチによる自動チャンネルプランによるチャンネル設定より優先されます。
Power	送信電力レベルは、アクセスポイントがどれだけ遠くまで RF 信号をブロードキャストできるかということに影響します。電力レベルが低すぎると、無線クライアントが信号を検出できなかったり、WLAN のパフォーマンスが低下します。逆に、電力レベルが高すぎると、RF 信号が通信範囲内の他のアクセスポイントとの間に干渉を起こす可能性が出てきます。 初期値「0」は AP プロファイルに設定されている送信電力レベルを使用することを意味しています。 注意 Valid AP データベース内に設定した送信電力レベルは固定され、アクセスポイントやスイッチによる自動送信電力調整の影響を受けることはありません。

第 6 章　D-Link アクセスポイントの保守管理

本章は以下の項により構成され、D-Link 統合アクセスシステムネットワーク上での D-Link アクセスポイントの保守管理に役立つ情報を示します。

項目	説明	参照ページ
アクセスポイントの再起動	D-Link 統合スイッチから、1 台または複数台のアクセスポイントを再起動します。	71 ページ
無線周波数帯の管理	チャンネルプランと自動電力調整の設定を行います。	71 ページ
アクセスポイントソフトウェアの更新	D-Link 統合スイッチにより管理下にあるアクセスポイントのソフトウェアを更新します。	75 ページ
高度なアクセスポイント管理	デバッグ機能を有効にして Telnet によりアクセスすることが可能にします。また、アクセスポイントの各無線インタフェースに対して、手動で RF チャンネルと送信電力を変更します。	77 ページ

CLI を使用してアクセスポイントの保守管理をするコマンドについての情報は「D-Link CLI MANUAL」を参照してください。

6.1 アクセスポイントの再起動

D-Link 統合スイッチから、1 台または複数台のアクセスポイントを再起動することができます。アクセスポイントを再起動する命令を送ると、アクセスポイントはハードウェアリセットする前に、スイッチとの間の SSL 接続を切断します。

アクセスポイントを再起動するためには、**WLAN タブ > Administration > AP Management > Reset** の順にメニューをクリックします。

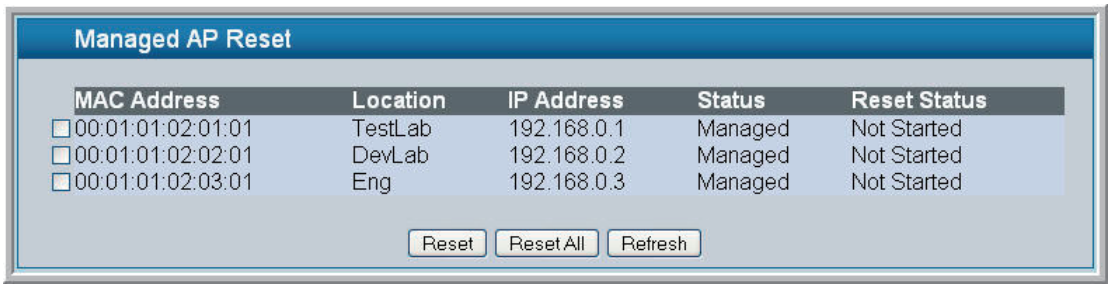


図 6-1　アクセスポイントの再起動

再起動するアクセスポイントを選択して「Reset」ボタンをクリックするか、または「Reset All」ボタンをクリックしてスイッチ管理下のすべてのアクセスポイントを再起動します。

アクセスポイントが再起動し、スイッチとの通信を再開するまでには数分かかります。再起動中にはアクセスポイントの状態は一度「failed」になりますが、オンライン状態に戻ると「Managed」に戻ります。

6.2 無線周波数帯の管理

無線周波数（RF）ブロードキャストチャンネルとは、アクセスポイント上の無線インタフェースが、データの送受信に使用する無線スペクトラムのある一部分を定義するものです。アクセスポイントが使用するためのチャンネル範囲は、アクセスポイントの IEEE 802.11 モード（バンドとも呼ばれる）により決定されます。

DWL-3500AP は 802.11g モードで動作するシングルバンドのシステムです。また DWL-8500AP は 802.11a と 802.11g モードで動作するデュアルバンドのシステムです。IEEE 802.11b と 802.11g モード（802.11b/g）は 2.4GHz 周波数帯で動作し、チャンネル 1 から 13 をサポートします。IEEE 802.11a モードは 5GHz 周波数帯で動作し、より広範囲で非連続のチャンネル（36、40、44、48、52、56、60、64）を使用します。

注意 使用可能なチャンネルはアクセスポイントが動作する国によって異なります。本項で説明するチャンネルは日本国において有効なものです。

干渉は、複数のアクセスポイントが互いの範囲内において、同一または重複するチャンネル上でブロードキャストする時に発生します。大量のデータや中継トラフィックが帯域獲得をめぐり争っているような高トラフィックの状況下において、干渉による影響は増大します。
「b/g」周波数帯の一般的な干渉ゼロのチャンネルセットは 1、6、11 です。チャンネル 1、4、8、11 の使用でオーバーラップを最低限に抑えることができます。干渉ゼロのチャンネルセットは「a」周波数帯でも存在しますが、「a」周波数帯のチャンネルは元々非連続でオーバーラップしていないため干渉を抑えることができます。

チャンネル計画と送信電力設定

D-Link 統合スイッチソフトウェアには、RF 干渉を最小限に抑えるために、各 D-Link アクセスポイントがどの RF チャンネルを使用すべきかを自動で判断する、チャンネルプランアルゴリズムを採用しています。チャンネルプランアルゴリズムを有効にすると、スイッチは管理下にある各アクセスポイントが使用しているチャンネルを定期的に評価し、干渉が認められる場合には、チャンネルを変更します。

注意 周波数およびチャンネルの設定に関する規則は、国によって異なります。802.11b/g においてチャンネル 1、6、11 をサポートしない国では、本チャンネルプランアルゴリズムは無効になります。日本や欧州の 802.11h 規格（DFS/ 動的周波数選択など）を規定している国では、802.11a の無線波において本アルゴリズムは無効です。

自動チャンネル選択アルゴリズムは、以下の条件に一致するアクセスポイントには影響を与えません。

- アクセスポイントへのチャンネル割り当てが、RADIUS サーバまたはローカル AP データベースで静的に行われた。
- アクセスポイントへのチャンネル割り当てが、「AP Management」の下の「Advanced」ページにより静的に行われた。
- アクセスポイントは **WLAN タブ > Administration > Advanced Configuration > AP Profiles** の「Radio」タブ内の「Automatic Channel」欄を無効に設定しているプロファイルを持っている（「Radio Configuration」の設定）。

さらに、Super A または Super G を設定している無線インタフェースにおいてはチャンネルプランアルゴリズムは使用できません。

注意 AP が固定チャンネルに割り当てられないか、または自動チャンネル選択アルゴリズムによって特定のチャンネルに割り当てられない場合、AP チャンネル選択モードは「最適」に設定されます。つまり、無線が再起動する時、または AP が電波信号を検出する場合、AP が「最適」なチャンネルを選択することを意味します。

RF 送信電力レベルは、アクセスポイントが RF 信号をブロードキャストできる距離に影響します。電力レベルが低すぎると、無線クライアントが信号を検出できなかったり、WLAN のパフォーマンスが低下したりします。逆に、電力レベルが高すぎると、RF 信号が通信範囲内の他のアクセスポイントとの間に干渉を起こす可能性が出てきます。また、物理的にビルやネットワークの枠を超えた RF 信号のブロードキャストは、ネットワークにセキュリティ上の危険をもたらします。

自動送信電力調整機能では、独自のアルゴリズムを使用して、RF 信号がなるべく遠くの無線クライアントまで到達し、かつ他のアクセスポイントがブロードキャストする RF 信号と干渉を起こすほど遠くまでは到達しないように、自動的に調整します。

チャンネルプランと自動電力調整の設定のためには、**WLAN タブ > Administration > AP Management > RF Management** の順にメニューをクリックします。

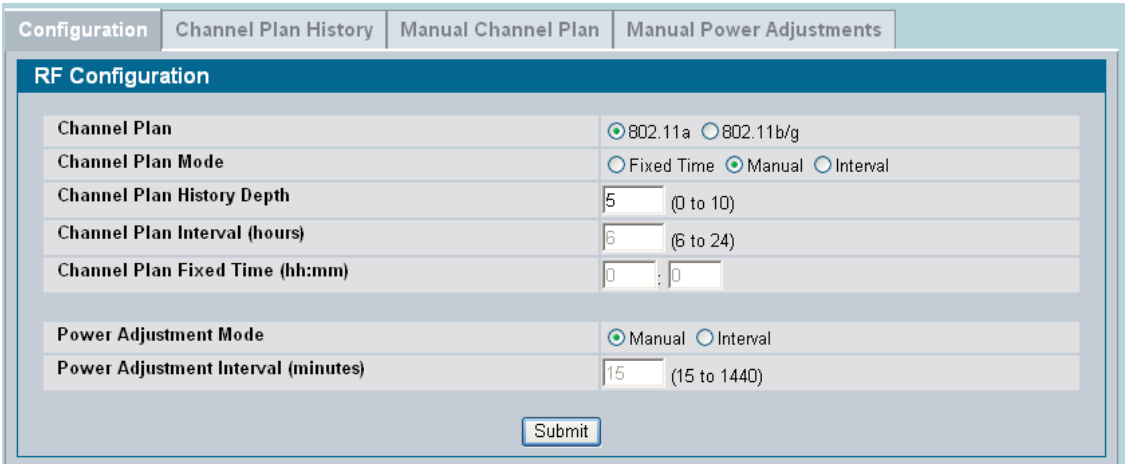


図 6-2　RF チャンネルプランと送信電力設定

表 6-1 は RF チャンネルプランと送信電力調整設定用の項目の詳細を示しています。

注意 アクセスポイントがチャンネル変更する時、接続中のすべての無線クライアントの接続は中断され、再接続が必要になります。再接続には数秒を要するため、音声や映像などの時間に依存するサービスに影響を与える場合があります。

表 6-1　RF チャンネルプランと送信電力調整

設定項目	説明
Channel Plan	チャンネルプランを設定する前に、無線モードを選択します。
Channel Plan Mode	チャンネル割り当てモードを選択します。 • Fixed Time - チャンネルプランの計算とチャンネル割り当ての時間を指定する必要があります。1 日のうちの指定した時刻に実行されます。 • Manual - チャンネルプランの計算と割り当てを手動で行うモードです。手動でチャンネルプランアルゴリズムを実行し、アクセスポイントに適用します。 • Interval - 本モードでは、スイッチは定期的にチャンネルプランの計算と適用します。実行間隔を 6~24 時間の間で指定します。「Submit」ボタンをクリックすると、実行時間までのカウントが始まります。
Channel Plan History Depth	チャンネルプランヒストリには、チャンネルプラン適用後にスイッチが各アクセスポイントに割り当てたチャンネルが記録されています。エントリは実行間隔、時間、またはチャンネルプランモードにかかわらず、ヒストリに追加されます。 ここで指定した数字により、チャンネル割り当ての繰り返し回数が制御されます。 **注意** チャンネル変更をしたアクセスポイントは、次回のサイクルではチャンネルは変更されません。本ヒストリにより同じアクセスポイントのチャンネルが何度も変更されることを防止します。例えば、「History Depth」が 3 に設定され、アクセスポイントが「Iteration」へのチャンネルを 1 に変更すると、必要な場合、チャンネル調整アルゴリズムの 5 回の反復サイクルの前にチャンネルを変更することはありません。

設定項目	説明
Channel Plan Interval (hours)	「Channel Plan Mode」欄で「Interval」を指定した場合、チャンネルプランの計算と割り当てを実行する間隔を指定します。単位は時間で、6~24 時間の間で指定します。
Channel Plan Fixed Time (hh: mm)	「Channel Plan Mode」欄で「Fixed Time」を指定した場合、チャンネルプランの計算と割り当てを実行する時刻を指定します。1 日のうちの本欄で指定した時刻に実行されます。
Power Adjustment Mode	アクセスポイントの無線送信電力は、AP プロファイル、ローカルデータベース、または RADIUS サーバで指定できます。AP プロファイルの送信電力レベルは、アクセスポイントの初期値のレベルであり、送信電力は AP プロファイルの値以下に調整はされません。 ローカルデータベースと RADIUS サーバでの設定は、常にプロファイルでの設定より優先されます。手動で送信電力をセットした場合は、その値が固定され、そのアクセスポイントでは自動送信電力アルゴリズムを使用できなくなります。 最大送信電力が、規制範囲（地域）やハードウェアの性能により、チャンネルに許可される最低の電力レベルになるように、最大送信電力のパーセンテージ（%）単位で設定できます。 • Manual - 本モードでは、管理者は「Manual Power Adjustments」ページから手動で電力調整を実行します。 • Interval - 本モードでは、スイッチが定期的に電力調整を計算し、すべてのアクセスポイントに適した送信電力を指示します。実行間隔は、「Submit」ボタンをクリックした時からカウントされます。 **注意** ローカルまたは RADIUS データベースに電力レベルを設定する場合、その値は AP プロファイルに設定した値より優先されます。 電力レベルの設定についての詳細は 57 ページの「5.3 無線電波の設定」および 69 ページの「5.5 Valid アクセスポイントの設定」を参照してください。
Power Adjustment Interval (minutes)	スイッチが電力調整アルゴリズムを実行する間隔を指定します。アルゴリズムは、「Power Adjustment Mode」欄で「Interval」を指定した場合のみ実行されます。

チャンネルプランヒストリの表示

D-Link 統合スイッチはアクセスポイントへのチャンネル割り当て情報を記録し、管理します。チャンネルプランヒストリ情報にアクセスするためには、**WLAN タブ > Administration > AP Management > RF Management** とクリックし、「Channel Plan History」タブを表示します。

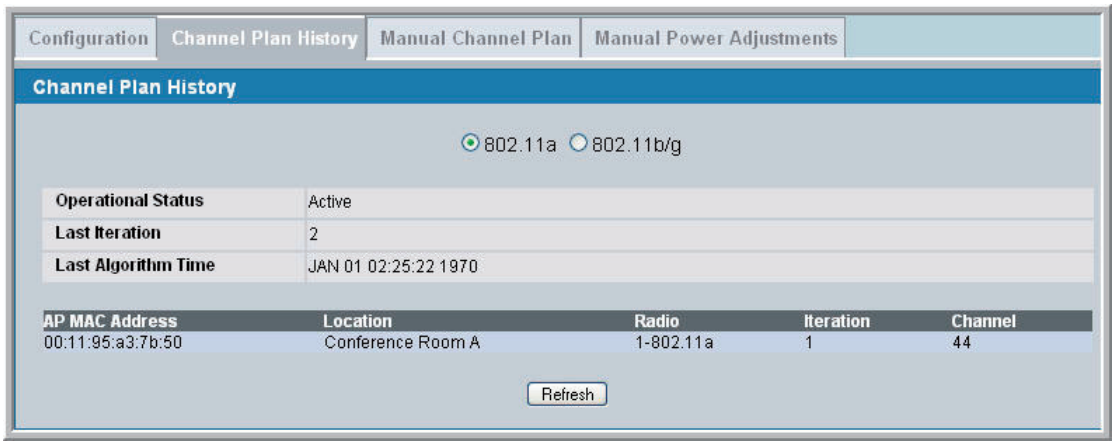


図 6-3　チャンネルプランヒストリ

表 6-2 にチャンネルプランヒストリの各設定項目の詳細を示します。

表 6-2　チャンネルプランヒストリ

設定項目	説明
802.11a または 802.11g	802.11a モードと 802.11g モードでは異なるチャンネルプランを使用します。そのためスイッチは別々にチャンネルヒストリを記録します。本ページに表示されるチャンネル情報は、802.11a か 802.11g のうち指定した方のどちらかになります。
Operational Status	スイッチが D-Link アクセスポイント上の指定無線モード上で自動チャンネル調整アルゴリズムを使用しているか否かを示します。
Last Iteration	チャンネルプラン調整された最後の反復サイクルを示します。 チャンネルを変更したアクセスポイントは、次回の反復サイクルではチャンネルは変更されません。これにより、同じアクセスポイントのチャンネルが何度も変更されることを防止します。 「AP Management」から「RF Management」をクリックして「Configuration」タブを選択して、「History depth」を設定することにより、記録・表示する最大反復サイクル回数を指定できます。
Last Algorithm Time	最後にチャンネルプランアルゴリズムが実行された日時を表示します。 **注意** システム時間を設定するためには、初期値では無効である SNTP の使用が必要になります。SNTP クライアントとサーバの設定は、Web インタフェースを使用して、「LAN」から「Administration」をクリックし、「SNTP Settings」ページで行います。CLI では「Global Config」モード内で sntp コマンドを実行します。
AP MAC Address Location Radio Iteration Channel	チャンネルプランの反復サイクルで、アクセスポイントに割り当てられたチャンネルを表示します。

手動チャンネルプランの起動

「Configuration」タブにおいて「Channel Plan Mode」に「Manual」を指定すると、「Manual Channel Plan」ページからチャンネルプランアルゴリズムを起動できるようになります。

手動でチャンネルプラン調整機能を実行するためには、チャンネルを調整する無線モード（802.11a または 802.11g）を指定して「Start」ボタンをクリックします。

図 6-4　手動チャンネルプラン

「Current Status」欄には以下のいずれかの状態が表示されます。

項目	説明
None	前回のスイッチの再起動からチャンネルプランアルゴリズムの手動による実行はありません。
Algorithm In Progress	チャンネルプランアルゴリズムを実行中です。
Algorithm Complete	チャンネルプランアルゴリズムは実行完了しました。表中にチャンネル割り当て案が表示されます。エントリにはアクセスポイントの現在のチャンネルおよび変更案が表示されます。変更案に同意し、変更を適用するためには「Apply」ボタンをクリックします。変更案の適用は手動で行います。
Apply In Progress	スイッチはチャンネルプランを適用し、表示されているアクセスポイントのチャンネル調整を行っています。
Apply Complete	アルゴリズムの実行およびチャンネル調整は完了しました。

チャンネルプランを実行すると、アルゴリズムによりチャンネルの変更が望ましいアクセスポイントが表示されます。「Current Channel」欄には現在使用しているチャンネルが、また「New Channel」欄には変更案が表示されます。変更案を実行するためには「Apply」ボタンをクリックします。アルゴリズムの実行後、どのアクセスポイントも表示されなければ、チャンネルの変更の必要がないことを示しています。

自動チャンネル選択が動作する時間と、チャンネル変更案を適用する時間の間に、ネットワークコンフィグレーションを変更することは可能です。

以下のような条件下では、アクセスポイントへのチャンネルの割り当てはできません。

- アクセスポイントがダウンしている。
- プロファイルのアップデートにより、アクセスポイントの無線モードが無効になっている。
- 無線モードにおいて無効なチャンネルが指定されている。
- チャンネルプランの計算後にアクセスポイントが再起動され、ローカルデータベースに静的に設定されたスタティックチャンネルを取得した。
- 「Advanced」ページによりチャンネルが手動で設定されている。
- アクセスポイントのプロファイルに自動チャンネルモードが無効に設定されている。

手動電力調整の起動

「Configuration」タブ上で「Power Adjustment Mode」を「Manual」に指定している場合、「Manual Power Adjustments」ページを使用して、送信電力調整アルゴリズムを手動で起動することができます。

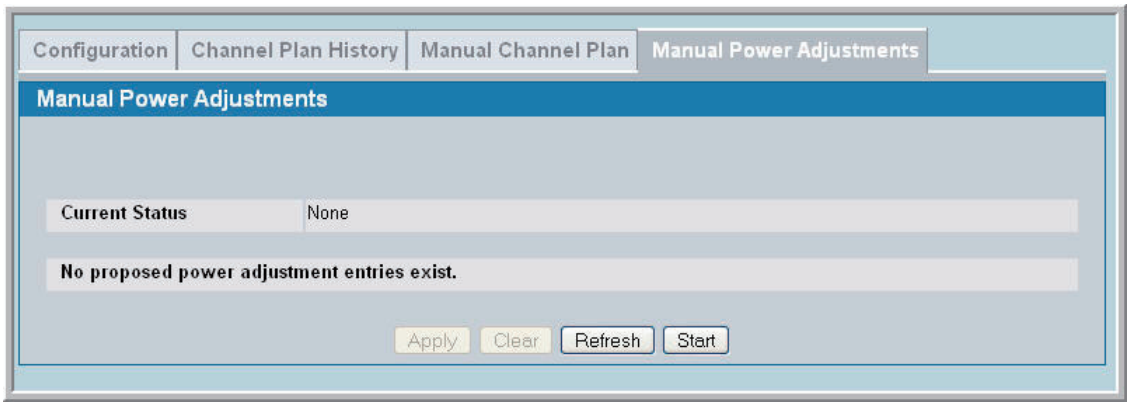


図 6-5　手動電力調整

「Current Status」欄には以下のいずれかの状態が表示されます。

項目	説明
None	前回のスイッチの再起動から電力調整アルゴリズムの手動による実行はありません。
Algorithm In Progress	電力調整アルゴリズムを実行中です。
Algorithm Complete	電力調整アルゴリズムは実行完了しました。表に電力調整案が表示されます。エントリにはアクセスポイントの現在の電力レベルおよび変更案が表示されます。変更案に同意し、変更を適用するためには「Apply」ボタンをクリックします。変更案の適用は手動で行います。
Apply In Progress	スイッチは表中に表示されているアクセスポイントを電力調整しています。
Apply Complete	アルゴリズムの実行および電力調整は完了しました。

6.3 アクセスポイントソフトウェアの更新

D-Link 統合スイッチにより管理下にあるアクセスポイントのソフトウェアを更新できます。1 台または複数の D-Link アクセスポイントを更新するためには、**WLAN タブ > Administration > AP Management > Software Download** の順にメニューをクリックし、以下の画面を表示します。

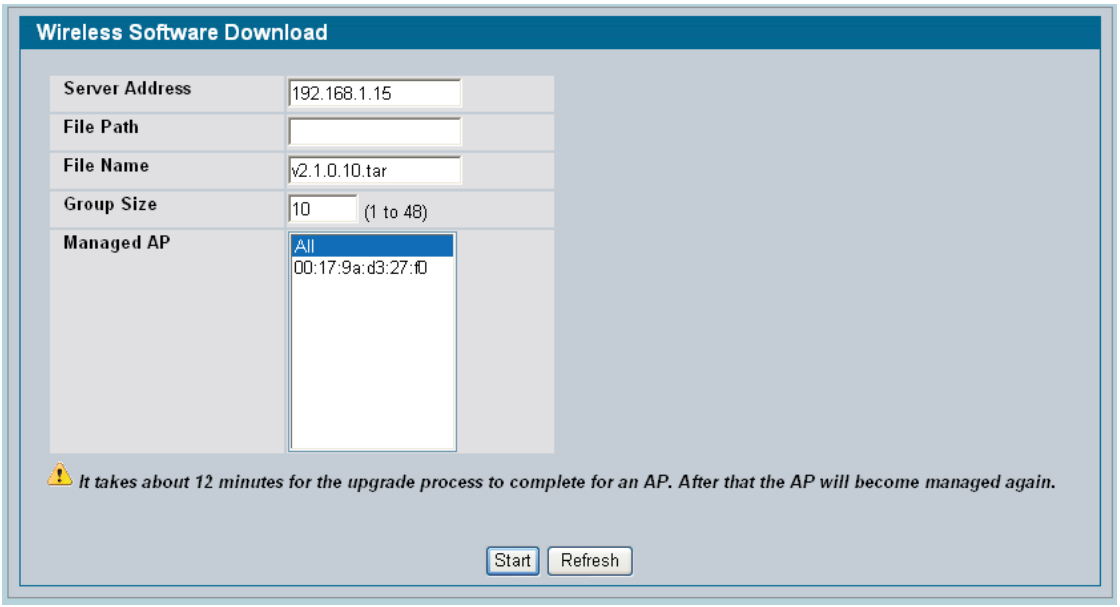


図 6-6　アクセスポイントの更新

注意 プログラムのダウンロードが完了すると、アクセスポイントは自動的に再起動します。

表 6-3 では、D-Link アクセスポイントを更新するために使用する各項目について説明します。

表 6-3　アクセスポイントの更新

設定項目	説明
Server Address	更新用ファイルが格納されているホストの IP アドレスを入力します。ホストには TFTP サーバがインストールされ、起動している必要があります。
File Path	更新用ファイルが格納されているディレクトリを入力します。96 文字まで入力できます。
File Name	更新用ファイルの名前を 32 文字までの半角英数字で入力します。拡張子「.tar」の入力が必要です。
Group Size	一度に更新するアクセスポイントの数。複数のアクセスポイントをアップグレードする場合、各アクセスポイントが TFTP サーバに接続してファイルをダウンロードします。TFTP サーバの過負荷防止のため、一度に更新するアクセスポイント数を制限できます。1 つのグループの更新後に、次のグループのアップグレードが開始されます。
Managed AP	プルダウンメニューにスイッチが管理するアクセスポイントが表示されます。 各アクセスポイントは MAC アドレスおよび設定されている場合にはロケーションによってで識別されます。1 台以上のアクセスポイントを更新する場合、プルダウンメニューから目的のアクセスポイントの MAC アドレスを選択します。全部のアクセスポイントを対象にする場合は、リストの一番上の「All」を選択します。「All」を選択すると、「Group Size」欄の入力により、同時に更新するアクセスポイントの数を制限して TFTP サーバの過負荷を防止します。 **注意** 更新は、すべてのアクセスポイントを対象にすることをお勧めします。

更新ファイルについての情報を入力後、「Start」ボタンをクリックして更新プロセスを開始します。新しい欄が表示され、更新の状況と結果を確認できます。

ソフトウェアのダウンロードは、「Abort」ボタンが表示されている時にだけ、すべての AP において進行中のコード転送を中止することができます。TFTP サーバからのダウンロードが完了していても、NVRAM を更新しません。一度、NVRAM の更新が関連する AP に対して始まると、「Abort」ボタンは見えなくなります。更新中、状態 / 経過を示すバーが表示されます。状態のバーは更新処理が完了すると表示されず、AP は起動し、管理されます。

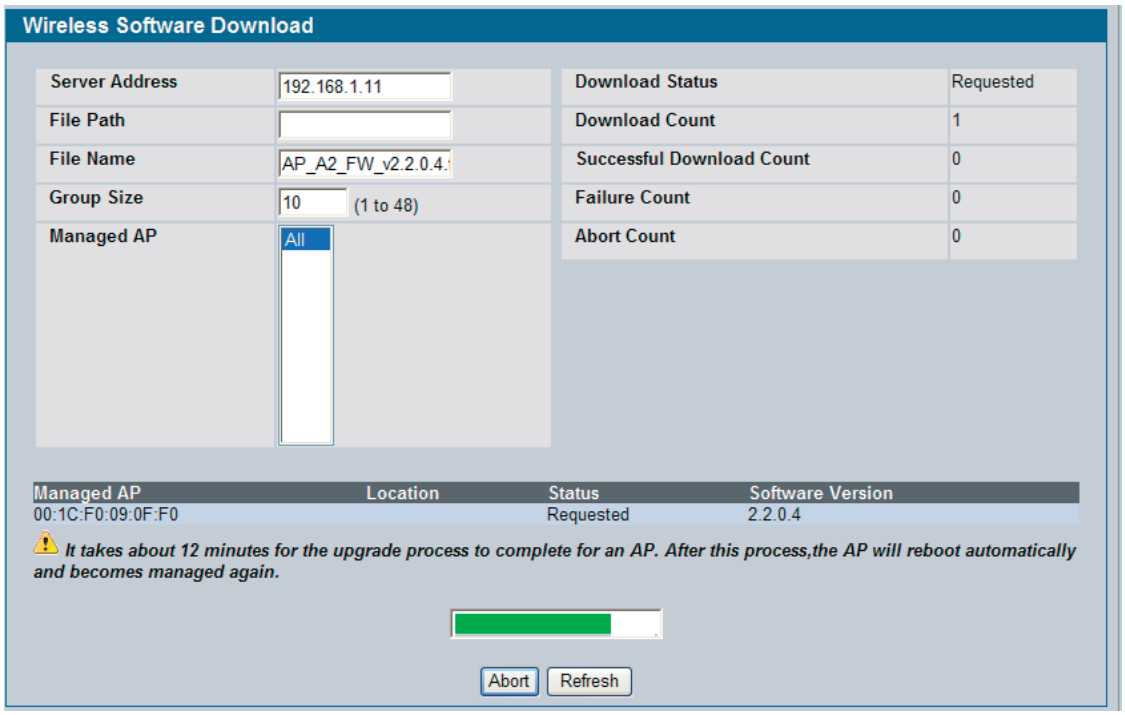


図 6-7　アクセスポイントアップグレード状況

表 6-4 に、アクセスポイントアップグレードプロセスを開始すると表示される項目について説明します。

表 6-4　アクセスポイントアップグレード状況

項目	説明
Status	すべてのアクセスポイントのアップグレードプロセスの状況を表示します。 • Not Started - 統合スイッチはダウンロードプロセスを開始していません。 • Requested - ソフトウェアダウンロードリクエストが発行されたが、スイッチはまだダウンロードをしていません。 • In Progress - 現在、AP はサーバからのソフトウェアダウンロードを試みています。 • Success - すべてのアクセスポイントのダウンロードが成功しました。TFTP サーバからアクセスポイントにソフトウェアが転送され、チェックサムで誤りが検出されなければ、アクセスポイントはスイッチにダウンロードの完了を報告します。プログラムはアクセスポイントのハードウェアプラットフォームに一致している必要があります。 • Failure - すべてのアクセスポイントでダウンロードに失敗しました。TFTP サーバに接続できなかった場合、アップグレード用ファイルを見つけられなかった場合、またはアクセスポイントとスイッチ間の接続を失った場合に、アクセスポイントはソフトウェアダウンロード失敗を報告します。

項目	説明
Download Count	ソフトウェアをダウンロードした、統合スイッチ管理下にあるアクセスポイントの数が表示されます。「Managed AP」欄に「All」を選択した場合は、ダウンロードリクエストを開始した時点で、統合スイッチの管理下にあったすべてのアクセスポイントの数が表示されます。1 台アップグレードしていれば、「1」と表示されます。
Success Count	新しいプログラムのダウンロードに成功したアクセスポイントの数が表示されます。はじめは「0」と表示されていますが、アクセスポイントがダウンロードに成功するごとに数値が増加していきます。
Failure Count	新しいプログラムのダウンロードに失敗したアクセスポイントの数が表示されます。はじめは「0」と表示されていますが、アクセスポイントがダウンロードに失敗するごとに数値が増加していきます。

同ページ中のリストに、アクセスポイントごとにダウンロードの状況とダウンロード中のソフトウェアのバージョンが表示されます。各アクセスポイントの「Status」欄には以下に示す状況の一つが表示されます。

項目	説明
Requested	ダウンロードリクエストが出されました。
Success	ダウンロードが成功しました。
Failure	ダウンロードが失敗しました。
Code Transfer In Progress	AP へのコードのダウンロードは進行中です。
NVRAM Update In Progress	AP NVRAM は更新済みです。
Waiting for APs to Download	コード伝送は完了しましたが、AP は、残りの AP のダウンロード終了を待ってから NVRAM の更新を開始します。

6.4 高度なアクセスポイント管理

D-Link アクセスポイントが「Managed」モードにある時は、アクセスポイントへのリモートアクセスはできなくなっています。しかし、**WLAN タブ > Administration > AP Management > Advanced** 画面で、デバッグ機能を有効にして Telnet によりアクセスすることが可能です。

「Advanced」画面から、アクセスポイントの各無線インタフェースに対して、手動で RF チャンネルと送信電力を変更することもできます。

図 6-8　高度なアクセスポイント管理

D-Link 統合スイッチによって管理されるアクセスポイントの MAC アドレスと場所が表示されます。場所は RADIUS またはローカルの有効 AP データベースの値に基づいています。

表 6-8 では、アクセスポイントに設定可能な高度な機能について説明します。

表 6-8　高度なアクセスポイント管理

設定項目	説明
Debug	トラブルシューティング用にアクセスポイントへの Telnet 接続を有効にし、CLI を使用してデバイスのデバッグを可能にします。以下のいずれかの状態を表示します。 • Disabled（無効） • Set Requested（リクエスト中） • Set in Progress（進行中） • Enabled（有効） 状態を変更するためには、「Debug」の状態のリンクをクリックして、「Managed AP Debug」ページを表示させます。表 6-9「Managed AP Debug」画面中の項目の詳細を説明します。
Channel	「Channel」のリンクをクリックすると「Managed AP Channel/Power Adjust」ページが表示され、Radio 1 と Radio 2 に対して新しいチャンネルを設定できます。使用できるチャンネルは、無線モードとアクセスポイントを使用する国によって異なります。表 6-10 に「Managed AP Channel/Power Adjust」ページの詳細を説明しています。
Power	「Power」のリンクをクリックすると「Managed AP Channel/Power Adjust」ページが表示され、アクセスポイントの送信電力を設定できます。表 6-10 に「Managed AP Channel/Power Adjust」ページの詳細を説明しています。

アクセスポイントのデバッグ機能を有効にする

デバッグ機能を有効にし、アクセスポイントに Telnet 接続可能な状態にできます。Telnet 接続後、コマンドを発行することで問題解決に利用できます。「Debug」の状態のリンクをクリックし、以下の「Managed AP Debug」画面を表示します。

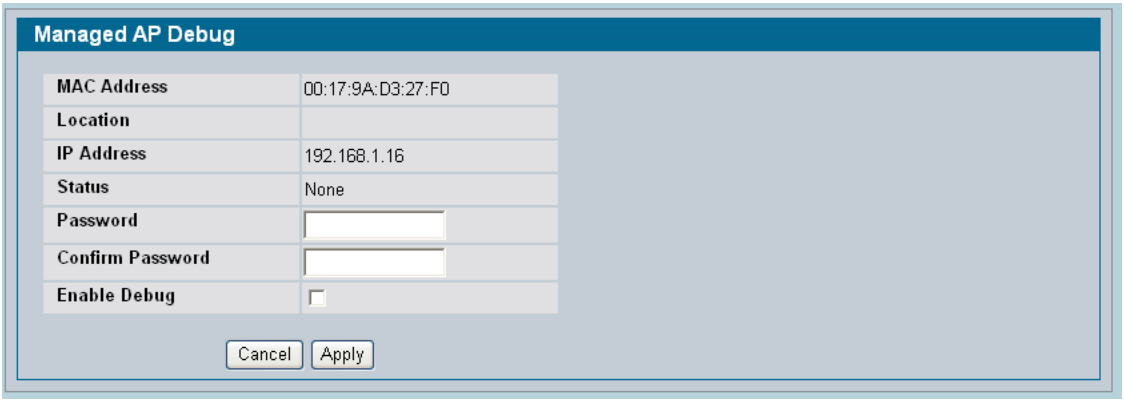


図 6-9　Managed AP Debug 管理

表 6-9　アクセスポイントのデバッグ

項目	説明
MAC Address	アクセスポイントの MAC アドレス。
Location	Valid AP データベースに登録されたアクセスポイントの場所。
IP Address	アクセスポイントの IP アドレス。
Status	デバッグ機能の状態。以下のいずれかが表示されます。 • None - デバッグ機能は有効、無効のいずれでもありません。 • Set Requested - デバッグ機能の状態を変更する要求が発行されています。 • Set Complete - デバッグ機能が有効または無効になりました。
Password	アクセスポイントの管理者用パスワードを入力します。初期値は「admin」です。
Confirm Password	確認のため、もう一度パスワードを入力します。
Enable Debug	本チェックボックスにより、デバッグ機能を有効または無効にします。チェックすると有効になります。 アクセスポイントに Telnet 接続すると、「AP interface login」プロンプトが表示されます。ユーザ名は「admin」です。上記「Password」欄に入力したパスワードを入力します。パスワードを変更していない場合、パスワードの初期値「admin」を使用します。アクセスポイントの CLI から、「!」を入力することにより、通常の Linux プロンプトにアクセスできます。 Linux OS プロンプト表示時には、以下のデバッグ用コマンドが実行できます。 • get management - 管理用インタフェースの情報を表示します。 • get managed-ap - 管理対象のアクセスポイントの情報を表示します。 • ifconfig - すべてのインタフェースを表示します。 • cat/proc/meminfo - メモリ使用率を表示します。

チャンネルと送信電力の調整

チャンネルと送信電力の変更は、動作中の変更に限定されます。チャンネルと送信電力の設定を変更しても、新しい変更内容はアクセスポイントまたはスイッチが再起動した時に失われます。

WLAN タブ > Administration > AP Management > Advanced をクリックし、「Managed AP Advanced」画面上で、現在の「Channel」または「Power」をクリックすると、以下の画面が表示されます。

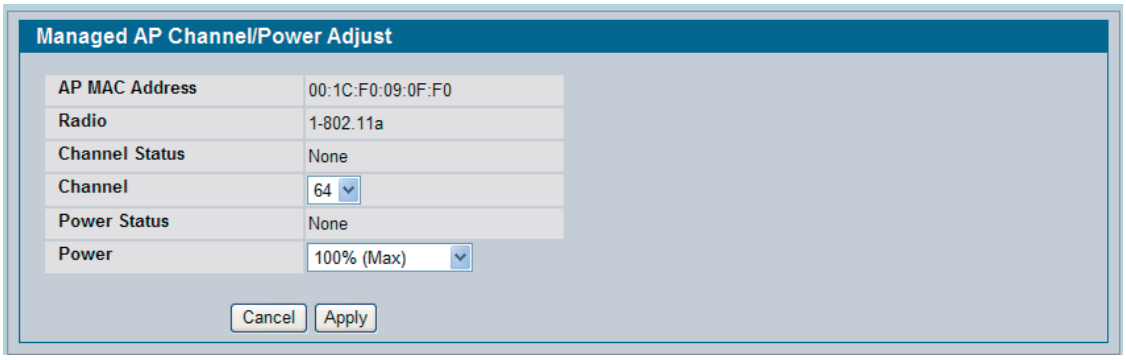


図 6-10　Managed AP Channel/Power Adjust 画面

表 6-10 「Managed AP Channel/Power Adjust」画面

項目	説明
AP MAC Address	アクセスポイントの MAC アドレスを示します。
Radio	無線インタフェースとモードを示します。変更はここで表示される無線インタフェースにだけ適用されます。
Channel Status	チャンネルの状態。以下のいずれかが表示されます。 • None - 以下のいずれでもない状態 • Set Requested - 変更リクエスト中 • Set Complete - 変更完了
Channel	チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。チャンネルの範囲や初期設定のチャンネルは無線インタフェースのモードにより異なります。 IEEE 802.11b/802.11g モードではチャンネル 1 から 13 を使用し、IEEE 802.11a モードではより広範囲で非連続のチャンネル群（36、40、44、48、52、56、60、64）を使用します。 注意 使用可能なチャンネルはアクセスポイントを使用する国によって異なります。 干渉は、複数のアクセスポイントが互いの範囲内において、同一または重複するチャンネル上でブロードキャストをする時に発生します。大量のデータや中継トラフィックが帯域獲得のために争っているような高トラフィックの状況下では、干渉による影響は増大します。 「Auto」を選択すると、アクセスポイントは RF エリア内の既に占有されているチャンネルをスキャンし、干渉のない、または空いているチャンネルを自動的に選択します。 チャンネルを指定する場合は、隣接するアクセスポイントが使用するチャンネルに干渉を与えないように注意してください。
Power Status	送信電力の状態。 • None - 以下のいずれでもない状態 • Set Requested - 変更要求中 • Set Complete - 変更完了
Power	送信電力レベルを 0%、5%（Max-9db）、25%（Max-6db）、50%（Max-3db）、100%（Max）から選択します。送信電力レベルは、アクセスポイントがどれだけ遠くまで RF 信号をブロードキャストできるかということに影響します。電力レベルが低すぎると、無線クライアントが信号を検知できなかったり、WLAN のパフォーマンスの低下が発生します。逆に、電力レベルが高すぎると、RF 信号が通信範囲内の他のアクセスポイントとの間に干渉を起こす可能性が出てきます。

第 7 章　状態および統計情報のモニタ

本章は以下の項で構成され、D-Link 統合アクセスシステムネットワークの状態および統計情報のモニタに役立つ情報を提供します。

項目	説明	参照ページ
無線グローバル情報のモニタ	スイッチや接続するデバイスの状況や統計情報をモニタします。	80 ページ
ピアスイッチの状態モニタ	ネットワーク上の他の D-Link 統合スイッチの情報を参照します。	82 ページ
全アクセスポイントのモニタ	検出したすべてのアクセスポイントの状態（管理下、接続失敗、不正等）を確認します。	83 ページ
管理対象アクセスポイントの状態モニタ	スイッチの管理下にある各アクセスポイントの各種情報を確認します。	84 ページ
アクセスポイント認証失敗状況の参照	D-Link 統合スイッチとの接続に失敗したアクセスポイントのリストを表示します。	96 ページ
不正アクセスポイントのモニタとアクセスポイントの RF スキャン	RF スキャンによって検出されたすべてのアクセスポイント（不正と報告されたものも含む）の情報を確認します。	97 ページ
接続中のクライアントのモニタ	スイッチ管理対象のアクセスポイントが接続中の無線クライアントについて、さまざまな情報を参照します	99 ページ
クライアント認証失敗状況の参照	アクセスポイントへの接続または認証に失敗した無線クライアントを表示します。	105 ページ
アドホッククライアントのモニタと管理	アドホックネットワークによって WLAN に接続しているクライアントを検索し、管理します。	106 ページ

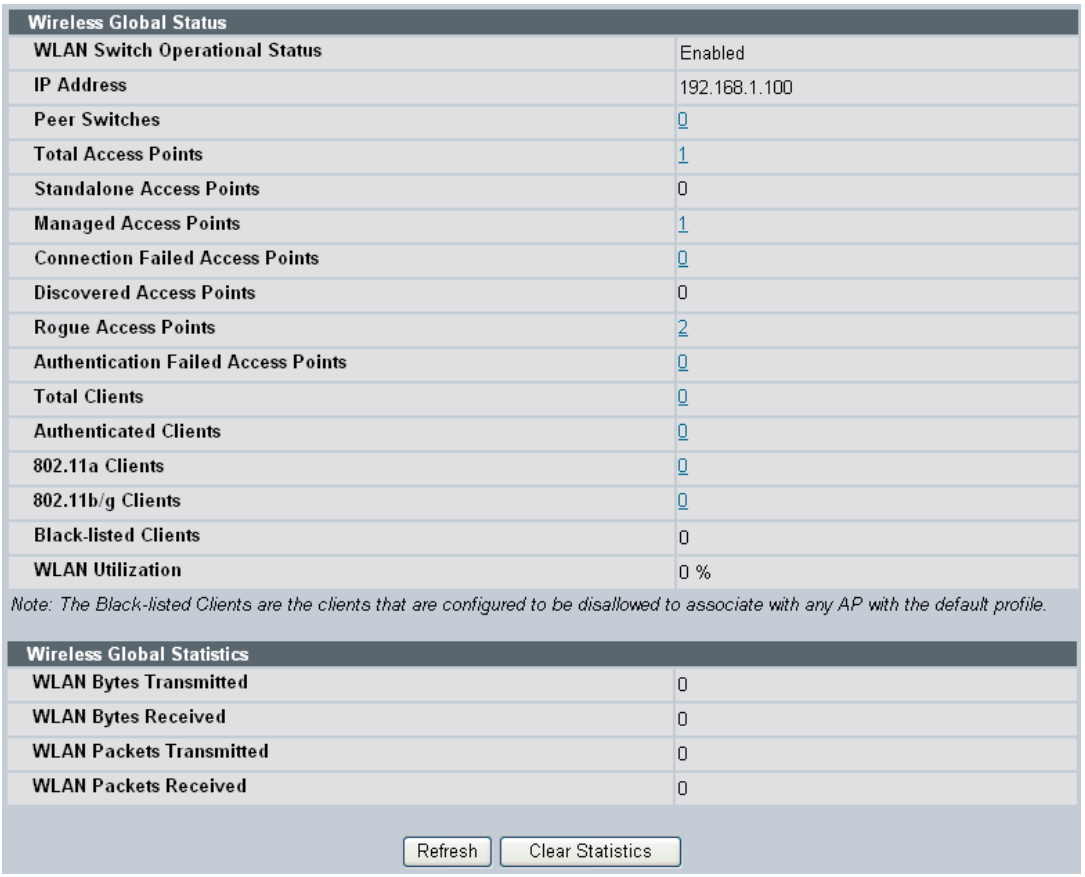
CLI を使用して、WLAN の状態と統計情報を確認するためのコマンドの詳細については、「D-Link CLI MANUAL」を参照してください。

7.1 無線グローバル情報のモニタ

D-Link 統合スイッチは、接続中の D-Link アクセスポイントやピアスイッチの情報を定期的に収集しています。「Global」ページを参照することにより、スイッチや接続するデバイスの状況や統計情報を参照できます。

WLAN 全体の統計情報にアクセスするためには、**WLAN タブ > Monitoring > Global** の順にメニューをクリックします。

「Wireless Global Status Statistics」ページの各項目の詳細情報を参照するためには、各値をクリックして、状態表示用のページにアクセスします。



Wireless Global Status

WLAN Switch Operational Status	Enabled
IP Address	192.168.1.100
Peer Switches	0
Total Access Points	1
Standalone Access Points	0
Managed Access Points	1
Connection Failed Access Points	0
Discovered Access Points	0
Rogue Access Points	2
Authentication Failed Access Points	0
Total Clients	0
Authenticated Clients	0
802.11a Clients	0
802.11b/g Clients	0
Black-listed Clients	0
WLAN Utilization	0 %

Note: The Black-listed Clients are the clients that are configured to be disallowed to associate with any AP with the default profile.

Wireless Global Statistics

WLAN Bytes Transmitted	0
WLAN Bytes Received	0
WLAN Packets Transmitted	0
WLAN Packets Received	0

Refresh　Clear Statistics

図 7-1　グローバル WLAN の状況

表 7-1 では「Wireless Global Status Statistics」ページ内の各項目について説明します。

表 7-1　グローバル WLAN の統計情報

項目	説明
WLAN Switch Operational Status	WLAN スイッチの動作状態が表示されます。WLAN スイッチが設定上有効になっていても、コンフィグレーション上の従属関係により、非稼働状態にある場合があります。稼働状態が無効である場合、その原因が続く「status」欄に表示されます。 WLAN スイッチは複数のコンポーネントで構成されています。システムの各コンポーネントが、それぞれ WLAN スイッチの動作状態（動作中 / 停止中）を認識する必要があります。動作状態の移行期間中には、動作状態は保留中と表示される場合があります。
IP Address	スイッチの IP アドレス。スイッチの IP アドレスについての情報は 39 ページの「スイッチと管理対象のアクセスポイントへの IP アドレスの割り当て」を参照してください。
Peer Switches	ネットワーク上で検出されたピア WLAN スイッチの数。
Total Access Points	データベース中の管理対象のアクセスポイントの総数。この値は常に「Managed Access Points」と「Connection Failed Access Points」と「Discovered Access Points」の値の和と等しくなります。
Standalone Access Points	検出された Standalone モードの D-Link アクセスポイントの合計数。Standalone モードの AP は、D-Link 統合スイッチで管理されません。
Managed Access Points	管理 AP データベース中のアクセスポイントの数。認証、設定がされており、無線スイッチとの間でアクティブな接続が確立されているアクセスポイントです。
Connection Failed Access Points	以前に認証され、スイッチの管理下にあったが、現在は無線スイッチとの間に接続が確立されていないアクセスポイントの数。
Discovered Access Points	スイッチと接続していますが、完全に設定されていない AP。この値には「検出」または「認証」状態のすべての管理 AP も含まれます。
Rogue Access Points	現在 WLAN 上で検出されているローグ（不正）アクセスポイントの数。アクセスポイントが RF スキャンする時、認知されていないアクセスポイントを検出する場合があります。このようなアクセスポイントをローグ（不正）として報告します。
Authentication Failed Access Points	統合スイッチにおいて、認証に失敗したアクセスポイント数。
Total Clients	データベース中のクライアントの総数。この値は「Associated」、「Authenticated」、「Disassociated」の状態のクライアントを含みます。
Authenticated Clients	クライアントデータベース中のクライアントで、「Authenticated」状態のクライアントの数。
802.11a Clients	802.11a 周波数帯で接続しているクライアントの数。
802.11b/g Clients	802.11b/g 周波数帯で接続しているクライアントの数。
Black-listed Clients	デフォルト AP プロファイルを使用するすべてのアクセスポイントとの接続を認められていないクライアントの数。
WLAN Utilization	本スイッチの管理下にあるすべてのアクセスポイントのネットワーク使用率。本値はグローバル統計値を基にしています。
WLAN Bytes Transmitted	本スイッチの管理下にあるすべてのアクセスポイントが送信した総データ量。単位はバイトです。
WLAN Bytes Received	本スイッチの管理下にあるすべてのアクセスポイントが受信した総データ量。単位はバイトです。
WLAN Packets Transmitted	本スイッチの管理下にあるすべてのアクセスポイントが送信したパケット数。
WLAN Packets Received	本スイッチの管理下にあるすべてのアクセスポイントが受信したパケット数。

IP 検出状態の確認

WLAN タブ > Monitoring > Global をクリックして「IP Discovery」タブを表示すると、**WLAN タブ > Administration > Basic Setup > Discovery タブ**の「IP List」にあるデバイスとの通信情報を確認できます。

図 7-2　無線検出状態

以下の状態の一つが表示されます。

項目	説明
Not Polled	スイッチは「L3/IP Discovery」リスト中の本 IP アドレスを持つデバイスに接続を試みていません。
Polled	スイッチは「L3/IP Discovery」リスト中の本 IP アドレスを持つデバイスに接続を試みました。
Discovered	スイッチは「L3/IP Discovery」リスト中の本 IP アドレスを持つデバイスに接続し、認証または認知しました。
Discovered-Failed	スイッチは「L3/IP Discovery」リスト中の本 IP アドレスを持つデバイスに接続したが、認証または認知に失敗しました。

デバイスがアクセスポイントであった場合は、そのエントリは失敗原因とともに「Authentication Failed Access Points」リストに表示されます。IP アドレスを「IP Discovery」リストに追加する方法については、43 ページの「スイッチにピアスイッチとアクセスポイントの IP アドレスを登録する」を参照してください。

7.2 ピアスイッチの状態モニタ

「Peer Switch Status」ページでは、ネットワーク上の他の D-Link 統合スイッチの情報を得ることができます。ピアスイッチの情報にアクセスするためには、**WLAN タブ > Monitoring > Peer Switch** の順にメニューをクリックします。

図 7-3　ピアスイッチの状態

同一ピアグループ内の、ピアスイッチ同士は、スイッチ、スイッチの配下のアクセスポイントおよびクライアントの情報を交換します。スイッチはそのデータをデータベースに保持するため、IP アドレスやソフトウェアバージョンなどのピア情報を確認することができます。スイッチとピアとの接続が切れると、すべてのピアスイッチの情報は削除されます。

ピアスイッチ同士は、配下のアクセスポイントについての設定プロファイルや追加情報の交換は行いません。つまり他のピアスイッチから自分の配下のアクセスポイントの状態や統計情報を見ることはできません。しかし、スイッチ同士はローグ（不正）アクセスポイント検出のための情報は共有しています。

表 7-2 は「Peer Switch Status」画面内の各項目の情報を示します。

表 7-2　「Peer Switch Status」ページ

項目	説明
IP Address	同一ピアグループ内のピアスイッチの IP アドレス。
Vendor ID	ピアスイッチのソフトウェアのベンダ ID
Software Version	ピアスイッチのソフトウェアバージョン
Protocol Version	ピアスイッチのプロトコルバージョン
Discovery Reason	ピアスイッチの検出方法。以下のいずれかが表示されます。 • L2 Poll • IP Poll
Age	前回の通信からの時間（時間 : 分 : 秒）

7.3 全アクセスポイントのモニタ

WLAN タブ > Monitoring > Access Point > All Access Points 画面を表示すると、検出したすべてのアクセスポイントの状態（管理下、接続失敗、不正等）を確認できます。

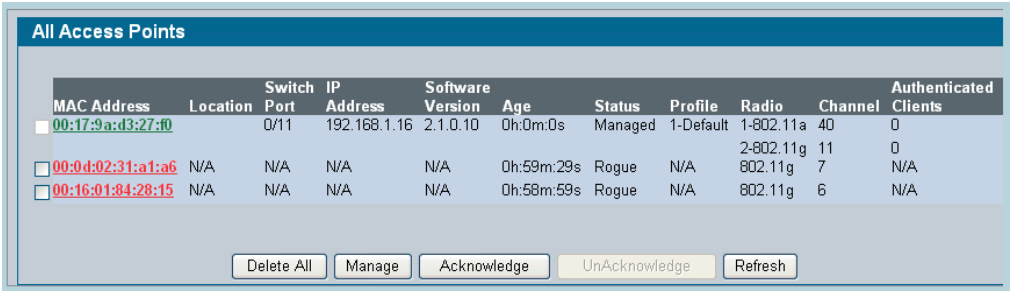


図 7-4　全アクセスポイント

リスト中のアクセスポイントの MAC アドレスの色により、以下の AP の状態を示しています。

項目	説明
緑	管理下にあるアクセスポイント。
赤	接続に失敗したアクセスポイント。
灰色	ローグ（不正）アクセスポイント。
橙	ピアマネージドアクセスポイント。

手動でステータスエントリを削除することができます。管理されているアクセスポイントを除いて、「All Access Points status」ページからすべての AP をクリアするためには、「Delete All」ボタンをクリックします。

不正アクセスポイントの次回検出時に、スイッチが管理する認証に失敗した AP を設定するため、MAC アドレスの左のチェックボックスを選択し、「Manage」ボタンをクリックします。「Valid Access Point Configuration」ページに表示されます。ローカルの Valid AP データベースに AP を保存するためには、AP を設定し、「Submit」ボタンをクリックします。アクセスポイントの認証に RADIUS サーバを使用している場合は、アクセスポイントの MAC アドレスを RADIUS サーバの AP データベースに登録する必要があります。詳細については、141 ページの「付録 B 外部 RADIUS サーバの設定」を参照してください。

アクセスポイントを認識済みのローグ（不正）として定義するためには、MAC アドレスの左のチェックボックスを選択し、「Acknowledge」ボタンをクリックします。スイッチはそのアクセスポイントを認識済みローグ（不正）として Valid AP データベースに追加します。アクセスポイントをローグ（不正）として定義するためには、認識済みの AP の MAC アドレスの左のチェックボックスを選択し、「UnAcknowledge」ボタンをクリックします。Valid AP データベースから AP を削除します。

検出されたアクセスポイントについての詳細情報を確認するためには、そのエントリの MAC アドレスをクリックしてください。

表 7-3 では「All Access Points」ページ内の各項目の情報を示します。

表 7-3　全アクセスポイントのモニタ

項目	説明
MAC Address	アクセスポイントの MAC アドレス。
Location	アクセスポイントの位置。Valid AP データベース（ローカルまたは RADIUS サーバ内）に登録されている値です。
Switch Port	同じ L3 ドメインに AP が直接的または間接的に接続しているスイッチ上の物理ポート（スロット / ポート形式）。 AP が L3 ネットワークの境界を越えている場合、「Unknown」が表示されます。
IP Address	アクセスポイントのネットワーク IP アドレス。
Software Version	アクセスポイントのソフトウェアバージョン。
Age	アクセスポイントの最後の検出および情報の更新からの経過時間。
Status	アクセスポイントの状態を示します。 • Managed - AP プロファイル設定が適用され、「managed」モードで動作中。 • No Database Entry - MAC アドレスがローカルまたは RADIUS サーバ内の Valid AP データベース中に存在しません。 • Authentication(Failed AP) - 統合スイッチまたは RADIUS サーバによる認証に失敗しました。 • Failed - 統合スイッチとの接続が失われました。エントリは管理者が削除するまでは管理 AP データベースに残ります。管理下のアクセスポイントは再起動中に「Failed」と表示されることがあります。 • Rogue - スイッチに接続を試みていません。またその MAC アドレスは Valid AP データベース内に存在しません。 • Acknowledged Rogue - 確認済みのローグ（不正）として認識されています。またその MAC アドレスは Valid AP データベース内に存在しています。

項目	説明
Profile	管理下のアクセスポイントに現在適用している AP プロファイル。プロファイルは Valid AP データベース内のアクセスポイントに適用されています。 注意 一度アクセスポイントが検出されて統合スイッチの管理下に入ると、その後プロファイルが Valid AP データベース内（ローカルまたは RADIUS サーバ）で変更されて新しいプロファイルが適用される場合、そのアクセスポイントは自動的に再起動します。
Radio	アクセスポイントの無線インタフェースが使用している無線モード。D-Link DWL-3500AP アクセスポイントは 1 つ、DWL-8500AP は 2 つの無線インタフェースを持ちます。
Channel	無線インタフェースで運用中のチャンネル。
Authenticated Clients	アクセスポイントのインタフェースに接続し認証されたクライアント数。

注意 「All Access Points」リストには AP に対するステータス値が不明なものも含まれています。そのような値は「N/A」と表記されます。

注意 Radio、Channel および Authenticated Clients を除きヘッダの列ごとに AP リストの順番を並び替えることができます。例えば、使用するプロファイルごとにアクセスポイントを並び替えたい場合は、「Profile」をクリックしてください。

7.4 管理対象アクセスポイントの状態モニタ

スイッチの管理下にある各アクセスポイントの各種情報を確認します。

WLAN タブ > Monitoring > Access Point > Managed Access Points の順にメニューをクリックします。次に「Status」タブをクリックすると、管理対象のアクセスポイントと隣接するアクセスポイントの設定情報や接続情報を確認できます。「Statistics」タブをクリックすると、各インタフェースにおいて送受信されたパケット数やデータ量が表示できます。

図 7-5 に 3 つの管理対象アクセスポイントが表示されている「Managed Access Point Status」ページの例を示します。

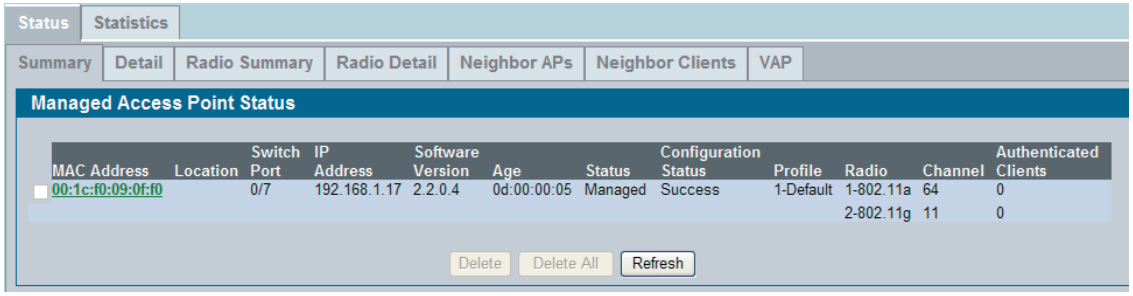


図 7-5　管理対象アクセスポイントの状態

「Managed Access Point Status」ページでは、以下のタブが使用できます。

タブ	説明
Summary	スイッチの管理下にあるアクセスポイントとそのサマリ情報を表示します。
Detail	アクセスポイントから収集した詳細情報を表示します。
Radio Summary	管理下にあるアクセスポイントの使用チャンネル、送信電力、および接続中のクライアント数を表示します。
Radio Detail	「Radio Summary」ページで、アクセスポイントの MAC アドレスをクリックすると無線インタフェースの詳細情報を参照できます。ラジオボタンをクリックすることにより、2 つの無線インタフェースから選択できます。
Neighbor APs	指定したアクセスポイントが、選択した無線インタフェース上で周期的な RF スキャンを行って検出した隣接アクセスポイントを表示します。
Neighbor Clients	アクセスポイントに接続中、またはアクセスポイントの当該無線インタフェースが検出したクライアントの情報を表示します。
VAP	選択したアクセスポイント上の仮想アクセスポイント（VAP）や、管理対象のアクセスポイントの無線インタフェースに関するサマリ情報を表示します。

表 7-4 に「Managed Access Point Status」ページの「Summary」タブ内の各項目について説明します。

表 7-4 「Managed Access Point Status」ページ「Summary」タブ

項目	説明
MAC Address	統合スイッチの管理下にあるアクセスポイントの MAC アドレス。
Location	アクセスポイントの位置。Valid AP データベース（ローカルまたは RADIUS サーバ内）に登録されている値です。
Switch Port	同じ L3 ドメインに AP が直接的または間接的に接続しているスイッチ上の物理ポート（スロット / ポート形式）。 AP が L3 ネットワークの境界を越えている場合、「Unknown」が表示されます。
IP Address	管理対象アクセスポイントのネットワーク IP アドレス。
Software Version	管理対象アクセスポイント上で運用中のソフトウェアのバージョン。
Age	統合スイッチとアクセスポイント間との最後の通信からの経過時間。
Status	アクセスポイントの状態を示します。以下のいずれかの状態が表示されます。 • Discovered - スイッチにより検出されましたが、認証はされていません。 • Authenticated - スイッチにより認可・認証されました（認証を有効に設定している場合）が、AP プロファイル設定が適用されていません。 • Managed - AP プロファイル設定が適用され、「managed」モードで動作中。 • Failed - 統合スイッチとの接続が失われました。エントリは管理者が削除するまでは管理 AP データベースに残ります。管理下のアクセスポイントは再起動中に「Failed」と表示されることがあります。
Configuration Status	アクセスポイントに対してプロファイルの設定が成功したかどうかを確認できます。以下の状態の一つが表示されます。 • Not Configured - アクセスポイントにプロファイルがまだ送信されていません。アクセスポイントが検出された可能性がありますが、まだ認証されていません。 • In Progress - スイッチからアクセスポイントに AP プロファイル・コンフィグレーションパケットを送信中です。 • Success - プロファイルがアクセスポイントに送信され、コンフィグレーションエラーは認められませんでした。 • Partial Success - AP プロファイルがアクセスポイントに送信されましたが、コンフィグレーションエラーが発生しました（例: コンフィグレーションパラメータが受け入れられない等）。ただし、アクセスポイントは運用可能です。 • Failure - AP プロファイルがアクセスポイントに送信されましたが、コンフィグレーションエラーが発生しました。アクセスポイントは運用不可です。
Profile	管理下のアクセスポイントに現在適用されている AP プロファイル。プロファイルは Valid AP データベース中においてアクセスポイントに適用されています。 **注意** 一度アクセスポイントが検出されて統合スイッチの管理下に入ると、その後プロファイルが Valid AP データベース内（ローカルまたは RADIUS サーバ）で変更され、新しいプロファイルが適用される場合、そのアクセスポイントは自動的に再起動します。
Radio	アクセスポイントの無線インタフェースが使用している無線モード。DWL-3500AP アクセスポイントは 1 つ、DWL-8500AP は 2 つの無線インタフェースを持ちます。
Channel	無線インタフェースで運用中のチャンネル。
Authenticated Clients	無線インタフェースでアクセスポイントに接続し認証されたクライアント数。

注意 リスト中のエントリの順番を、欄の項目ごとに並び替えることができます。例えば、使用するプロファイルごとにアクセスポイントを並び替えたい場合は、「Profile」をクリックしてください。

管理対象アクセスポイントの詳細な状態を確認する

スイッチの管理下にあるアクセスポイントの詳細な情報を得るには、「Detail」タブ内の表の上部にあるプルダウンメニューから、目的のアクセスポイントの MAC アドレスを選択します。アクセスポイントを再起動するためには、「Reset」ボタンをクリックします。再起動を本当に行うかを確認するポップアップ画面が表示されます。再起動する場合は、「OK」ボタンをクリックします。

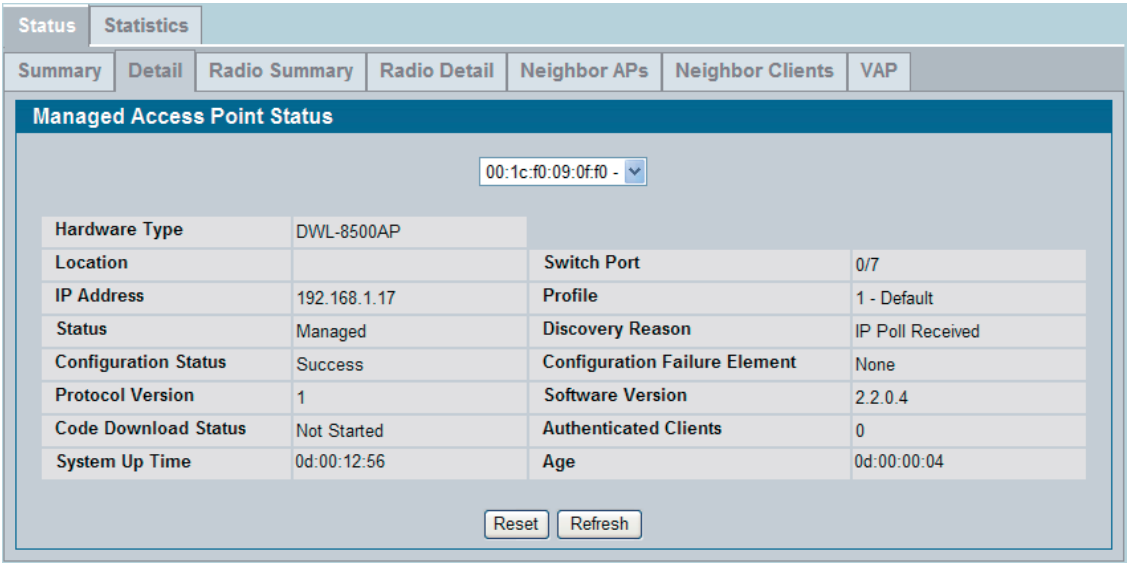


図 7-6 「Managed Access Point Status」ページの「Detail」タブ

再起動を行うと、アクセスポイントに接続中のクライアントはすべて切断されます。アクセスポイントの状態データを更新するためには「Refresh」ボタンをクリックします。

表 7-5 に「Managed Access Point Status」ページの「Detail」タブ内の各項目について説明します。

表 7-5 「Managed Access Point Status」ページ「Detail」タブ

項目	説明
MAC Address- Location	表の上部のラベルはアクセスポイントの MAC アドレスおよび場所を示しています。場所は Valid AP データベースに設定されている値です。プルダウンメニューから詳細データを表示する MAC アドレスを選択します。
Hardware Type	AP のハードウェアタイプ。DWL-8500AP か DWL-3500AP のいずれか。
Switch Port	同じ L3 ドメインに AP が直接的または間接的に接続しているスイッチ上の物理ポート（スロット / ポート形式）。 AP が L3 ネットワークの境界を越えている場合、「Unknown」が表示されます。
IP Address	管理対象アクセスポイントのネットワーク IP アドレス。
Profile	管理下のアクセスポイントに現在適用されている AP プロファイル。プロファイルは Valid AP データベース内のアクセスポイントに適用されています。 **注意** 一度アクセスポイントが検出され、統合スイッチの管理下に入ると、その後プロファイルが Valid AP データベース内（ローカルまたは RADIUS サーバ）で変更され、新しいプロファイルが適用される時、そのアクセスポイントは自動的に再起動します。
Status	アクセスポイントの状態を示します。以下の状態の一つが表示されます。 • Discovered - スイッチにより検出されましたが、認証されていません。 • Authenticated - スイッチにより認可・認証されました（認証を有効に設定している場合）が、AP プロファイル設定が適用されていません。 • Managed - AP プロファイル設定が適用され、「managed」モードで動作中。 • Failed - 統合スイッチとの接続が失われました。エントリは管理者が削除するまでは管理 AP データベースに残ります。管理下のアクセスポイントは再起動中に「Failed」と表示されることがあります。
Discovery Reason	アクセスポイントを検出した方法を表示します。以下の一つが表示されます。 • IP Poll Received - 統合スイッチからの IP ポーリングにより検出。その IP アドレスは IP ポーリングリスト内に設定されています。 • Peer Redirect - ピアスイッチからのリダイレクトにより検出。アクセスポイントは他のピアスイッチへの接続を試みたが、そのピアスイッチから現在接続中の統合スイッチの IP アドレスを取得した（アクセスポイントを認可する時、ピアは統合スイッチ IP アドレスを RADIUS サーバからの応答により取得）。 • Switch IP Configured - アクセスポイントに統合スイッチの IP アドレスが設定されていた。 • Switch IP DHCP - アクセスポイントは統合スイッチの IP アドレスを DHCP オプション 43 から取得した。 • L2 Poll Received - D-Link 無線デバイス検出プロトコルにより検出された。

項目	説明
Configuration Status	アクセスポイントに対してプロファイルの設定が成功したかどうかを確認できます。以下の状態の一つが表示されます。 • Not Configured - アクセスポイントにプロファイルがまだ送信されていません。アクセスポイントが検出された可能性がありますが、まだ認証されていません。 • In Progress - スイッチからアクセスポイントに AP プロファイル・コンフィグレーションパケットを送信中です。 • Success - プロファイルがアクセスポイントに送信され、コンフィグレーションエラーは認められませんでした。 • Partial Success - AP プロファイルがアクセスポイントに送信されましたが、コンフィグレーションエラーが発生しました（例 : コンフィグレーションパラメータが受け入れられない等）。ただし、アクセスポイントは運用可能です。 • Failure - AP プロファイルがアクセスポイントに送信されましたが、コンフィグレーションエラーが発生しました。アクセスポイントは運用不可です。
Protocol Version	アクセスポイントがサポートするプロトコルのバージョン。アクセスポイントの検出の際に取得される情報です。
Software Version	アクセスポイントのソフトウェアバージョン。アクセスポイントの検出の際に取得される情報です。
Last Failing Configuration Element	「Configuration Status」欄で「Partial Success」、「Complete Failure」が表示されている場合、コンフィグレーション中に失敗した最後のエレメントが表示されます。本情報は、失敗したエレメントがある時に表示されます。
Configuration Failure Error Message	「Configuration Status」欄で「Partial Success」、「Complete Failure」が表示されている場合、アクセスポイントから取得に失敗したエレメントについてのエラーメッセージを含む ASCII 文字情報が表示されます。
Code Download Status	アクセスポイントへのソフトウェアのダウンロードリクエストの状態を示します。以下の状態の一つが表示されます。 • Not Started - アクセスポイントへのソフトウェアのダウンロードはリクエストされていない。 • Requested - アクセスポイントへのソフトウェアのダウンロードがリクエストされたが、スイッチはまだ処理していない。 • In Progress - スイッチはアクセスポイントへのソフトウェアのダウンロードを処理中である。 • Success - アクセスポイントは新規ソフトウェアのダウンロードに成功した。 • Failure - アクセスポイントは新規ソフトウェアのダウンロードに失敗した。
Associated Clients	アクセスポイントに現在接続しているクライアントの総数。この値は、アクセスポイント上で動作中のすべての VAP に接続しているクライアントの和です。
Authenticated Clients	現在アクセスポイントに認証されているクライアントの総数。この値は、アクセスポイント上で動作中のすべての VAP に認証されたクライアントの和です。
System Up Time	前回のアクセスポイントのパワーオンリセットからの経過時間。単位は秒。
Age	統合スイッチとアクセスポイント間の最後の通信からの経過時間。

管理対象アクセスポイントの無線サマリ情報の参照

スイッチ管理下のアクセスポイント上で動作する各無線インタフェースに関する一般情報を参照することができます。「Managed Access Point Radio Summary」ページでは、すべての管理対象アクセスポイントについてチャンネル、送信電力、および接続中のクライアントの情報を確認できます。特定のアクセスポイント上の無線インタフェースに関する詳細情報は、該当する無線インタフェースをクリックして表示してください。

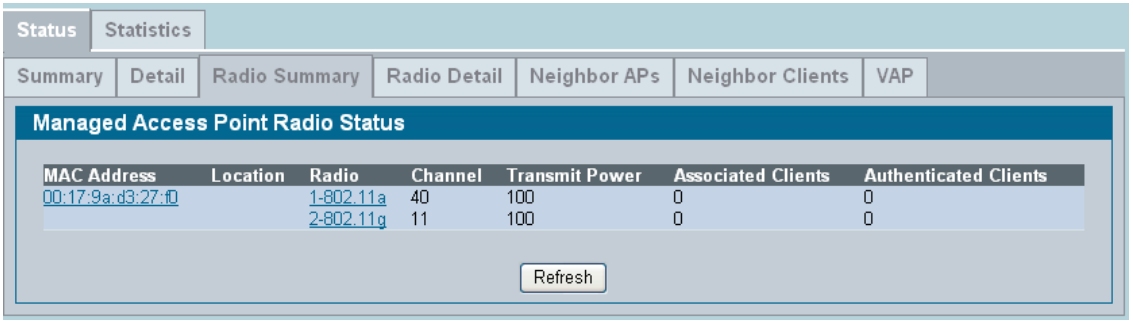


図 7-7 「Managed Access Point Status」ページの「Radio Summary」タブ

表 7-6 に「Managed Access Point Status」ページの「Radio Summary」タブ内の各項目について説明します。

表 7-6 「Managed Access Point Status」ページ「Radio Summary」タブ

項目	説明
MAC Address	統合スイッチの管理するアクセスポイントの MAC アドレス。
Location	アクセスポイントの位置。Valid AP データベース（ローカルまたは RADIUS サーバ内）に設定されている値です。
Radio	無線インタフェース、および設定された無線モードを表示します。無線インタフェースが無効の場合、「Off」と表示されます。
Channel	無線インタフェースが有効である場合は、使用中のチャンネルが表示されます。
Transmit Power	無線インタフェースが有効である場合は、現在の送信電力が表示されます。
Associated Clients	指定した無線モードで有効な VAP に接続中のクライアントの総数。
Authenticated Clients	アクセスポイントに接続し、認証されたクライアントの数。指定した無線モードで有効な VAP に認証されたクライアントの総数。

管理対象アクセスポイントの無線詳細情報の参照

スイッチの管理対象であるアクセスポイント上の無線インタフェースに関する詳細情報は、「Managed Access Point Status」ページの「Radio Detail」タブで参照することができます。

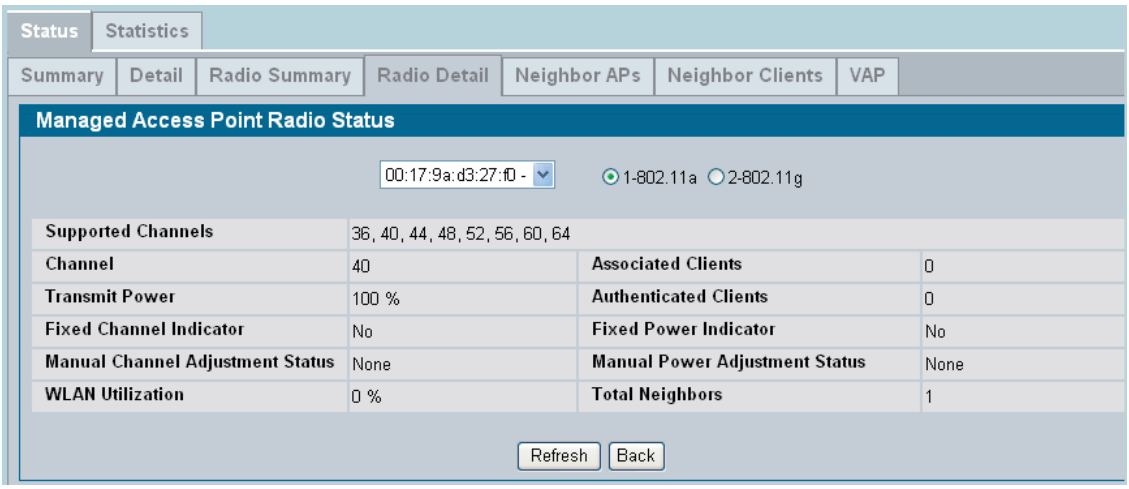


図 7-8 「Managed Access Point Status」ページの「Radio Detail」タブ

表 7-7 に「Managed Access Point Status」ページの「Radio Detail」タブ内の各項目について説明します。

表 7-7「Managed Access Point Status」ページ「Radio Detail」タブ

項目	説明
MAC Address - Location (プルダウンメニュー)	アクセスポイントの MAC アドレスと場所。プルダウンメニューから選択したアクセスポイントの詳細情報を表示します。
Radio	無線インタフェースおよび設定された無線モード。無線インタフェースが無効に設定されていれば、無線モードには、設定されているモードの代わりに「Off」と表示されます。
Supported Channels	アクセスポイントがスイッチに報告する、チャンネル割り当ての候補となるチャンネル。リスト中のエントリは国コード、ハードウェアの性能、および設定によるチャンネル制限により異なります。
Channel	無線インタフェースが有効な場合、現在動作状態にあるチャンネルが表示されます。
Associated Clients	指定した無線モードで有効な VAP に接続中のクライアントの総数。
Authenticated Clients	アクセスポイントに接続し、認証されたクライアントの数。指定した無線モードで有効な VAP に認証されたクライアントの総数。
Transmit Power	無線インタフェースが有効である場合は、現在の送信電力が表示されます。
Fixed Channel Indicator	本フラグは固定チャンネルが設定され、無線インタフェースに割り当てられているかを示しています。固定チャンネルは Valid AP データベース（ローカルまたは RADIUS サーバ）において設定できます。
Fixed Power Indicator	本フラグは固定送信電力が設定され、無線インタフェースに割り当てられているかを示しています。固定送信電力は Valid AP データベース（ローカルまたは RADIUS サーバ）において設定できます。
Manual Channel Adjustment Status	チャンネル変更する手動リクエストの現在の状況を示しています。以下のいずれかが表示されます。 • Not Started - チャンネル変更のリクエストは発行されていません。 • Requested - ユーザによりチャンネル変更のリクエストが発行されたが、スイッチはまだ処理をしていません。 • In Progress - スイッチはチャンネル変更リクエストを処理中です。 • Success - チャンネル変更リクエストは完了しました。 • Failure - チャンネル変更リクエストは失敗しました。
Manual Power Adjustment Status	送信電力変更する手動リクエストの現在の状況を示しています。以下のいずれかが表示されます。 • Not Started - 電力変更のリクエストは発行されていません。 • Requested - ユーザにより電力変更のリクエストが発行されたが、スイッチはまだ処理をしていません。 • In Progress - スイッチは電力変更リクエストを処理中です。 • Success - 電力変更リクエストは完了しました。 • Failure - 電力変更リクエストは失敗しました。
WLAN Utilization	物理帯域でのネットワーク使用率の合計を示します。値は無線統計情報を元にしています。
Total Neighbors	RF エリア内の指定帯域内で隣接するデバイス（アクセスポイントとクライアントの両方）の数。

管理対象アクセスポイントの隣接アクセスポイントの参照

RF スキャン中、アクセスポイントは隣接アクセスポイントから送信されているビーコン情報を収集し保存しています。アクセスポイントは、最大 64 台の隣接アクセスポイントの情報を保存できます。隣接スキャン情報が許容量を超えると、古いデータは上書きされます。

「Neighbor Clients」タブをクリックし、「Managed Access Point Neighbor AP Status」画面を表示します。
「Delete All Neighbors」ボタンをクリックすると、リスト内のデータをすべて削除します。削除後は、新規に検出された隣接アクセスポイントの情報を書きます。

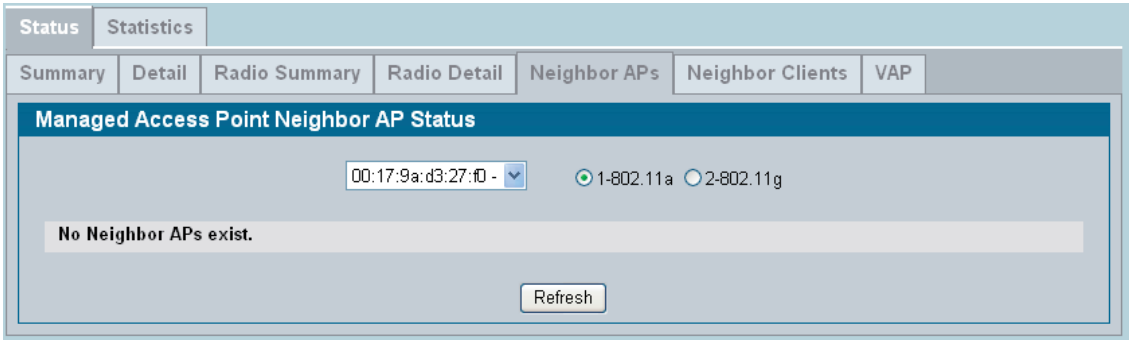


図 7-9 「Managed Access Point Status」ページの「Neighbor APs」タブ

表 7-8 に「Managed Access Point Status」ページの「Neighbor APs」タブ内の各項目について説明します。

表 7-8 「Managed Access Point Status」ページ「Neighbor APs」タブ

項目	説明
MAC Address-Location (プルダウンメニュー)	アクセスポイントの MAC アドレスと場所。プルダウンメニューから選択したアクセスポイントの詳細情報が表示されます。
Radio （例 : 1-802.11g）	無線インタフェースと設定された無線モード。無線インタフェースを選択すると、その無線インタフェースにおいて RF スキャンによって検出された隣接アクセスポイントを表示します。
Neighbor AP MAC	隣接アクセスポイントネットワークの MAC アドレス。物理的な無線インタフェースまたは VAP の MAC アドレス。D-Link アクセスポイントの場合は常に VAP の MAC アドレスです。隣接アクセスポイントの MAC アドレスは、RF スキャン状態の内容と相互参照できます。
SSID	隣接アクセスポイントネットワークの SSID
RSSI	受信信号強度表示信号。隣接アクセスポイントからの信号強度を示します。これにより、管理対象のアクセスポイントと隣接アクセスポイント間の距離が推測できる場合があります。
Status	隣接アクセスポイントの管理状況を示します。スイッチに認識されている有効なアクセスポイントであるか、またはローグ（不正）と見なされるかなどの情報を得ることができます。以下のいずれかが表示されます。 • WS Managed - 本隣接アクセスポイントは、本スイッチの管理下にあります。アクセスポイントの状態は MAC アドレスにより参照できます。 • Peer WS Managed - 本隣接アクセスポイントは、同一ピアグループ内の他のスイッチにより管理されています。 • Acknowledged Rogue - 本隣接アクセスポイントは、Valid AP エントリとしてローカルまたは RADIUS サーバに登録されています。認証され、不正アクセスポイントとの報告はされていません。 • Ad Hoc Rogue - 本隣接アクセスポイントはアドホックネットワークに参加していることが検知されました。
Age	無線インタフェースにおいて、本アクセスポイントが RF スキャンによって最後に報告されてからの経過時間。

隣接アクセスポイントに接続中のクライアントの参照

「Neighbor Clients」タブを使用すると、指定したアクセスポイントにより検出された無線クライアントの情報を表示します。D-Link アクセスポイントは 1024 台のクライアントの情報を保存できます。クライアントの情報が許容量を超えると、古いデータから上書きされます。「Delete All Neighbors」ボタンをクリックすると、リスト内のデータをすべて削除します。削除後は、新規に検出された隣接アクセスポイントの情報が書かれ、接続するクライアントが検出されます。ステータスを更新するためには、「Refresh」ボタンをクリックします。

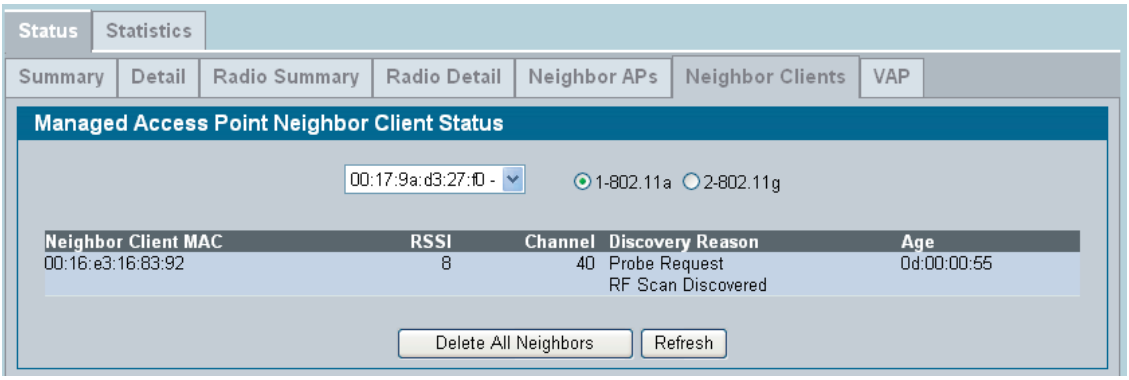


図 7-10 「Managed Access Point Status」ページの「Neighbor Clients」タブ

表 7-9 に「Managed Access Point Status」ページの「Neighbor Clients」タブ内の各項目について説明します。

表 7-9 「Managed Access Point Status」ページ「Neighbor Clients」タブ

項目	説明
MAC Address-Location (プルダウンメニュー)	アクセスポイントの MAC アドレスと場所。プルダウンメニューから選択したアクセスポイントの詳細情報が表示されます。
Radio（例 : 1-802.11g）	無線インタフェースと設定された無線モード。無線インタフェースを選択すると、その無線インタフェースで RF スキャンによって検出された隣接クライアントを表示します。
Neighbor Client MAC	隣接クライアントの MAC アドレス。
RSSI	受信した信号強度検出。隣接クライアントからの信号強度を示します。これにより、管理対象のアクセスポイントと隣接クライアント間の距離が推測できる場合があります。
Channel	クライアントからのフレームを受信した管理対象のアクセスポイントのチャンネル。本インタフェースの運用チャンネルとは異なる場合があります。
Discovery Reason	隣接クライアントの検出原因。複数の原因が表示される場合があります。 • RF Scan - 本隣接クライアントは、RF スキャンにより報告されました。RF スキャンによるクライアント検出は困難なため、通常は本原因以外が表示されます。 • Probe Request - 管理対象のアクセスポイントが本隣接クライアントからプローブリクエストを受信しました。 • Associated to Managed AP - 本隣接クライアントは、当スイッチ管理下の他のアクセスポイントと接続しています。 • Associated to this AP - 本隣接クライアントは、当アクセスポイントと接続しています。 • Associated to Peer AP - 本隣接クライアントは、ピアスイッチ管理下のアクセスポイントと接続しています。 • Ad Hoc Rogue - 本隣接クライアントはアドホックネットワークに参加していることが検知されました。
Age	無線インタフェースで本隣接クライアントが RF スキャンにより最後に報告されてからの経過時間。

管理対象アクセスポイントの仮想アクセスポイントの参照

1 台のアクセスポイントの各インタフェースに対して 8 つまでの仮想アクセスポイント（VAP）を設定できます。スイッチの管理下にあるアクセスポイントの各無線インタフェースに設定した VAP の設定サマリ情報、および各 VAP に接続中のクライアントの数を表示することができます。

「VAP」タブをクリックし、「Managed Access Point VAP Status」を表示します。

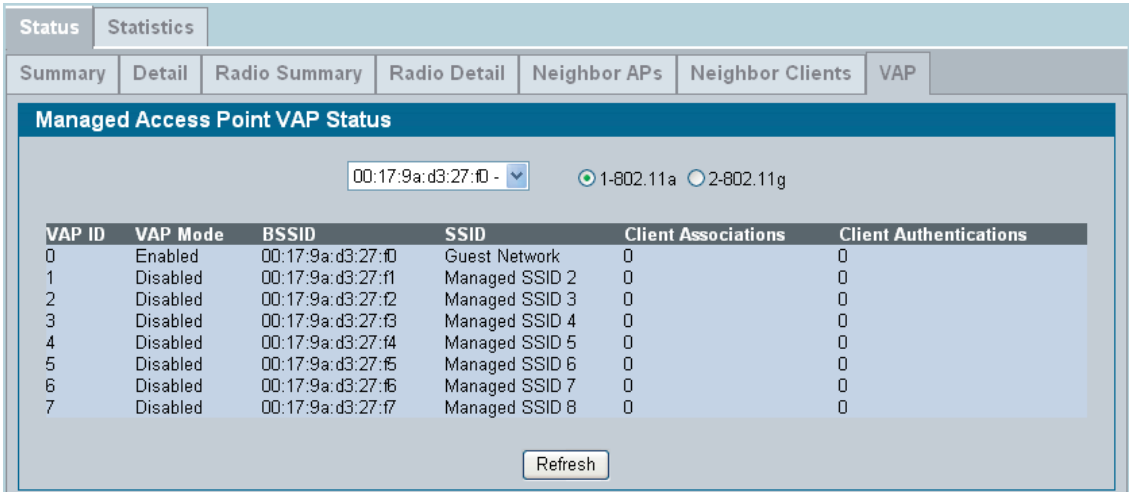

Status
Statistics
Summary
Detail
Radio Summary
Radio Detail
Neighbor APs
Neighbor Clients
VAP
Managed Access Point VAP Status
00:17:9a:d3:27:f0 -
1-802.11a
2-802.11g
VAP ID VAP Mode BSSID SSID Client Associations Client Authentications
0 Enabled 00:17:9a:d3:27:f0 Guest Network 0 0
1 Disabled 00:17:9a:d3:27:f1 Managed SSID 2 0 0
2 Disabled 00:17:9a:d3:27:f2 Managed SSID 3 0 0
3 Disabled 00:17:9a:d3:27:f3 Managed SSID 4 0 0
4 Disabled 00:17:9a:d3:27:f4 Managed SSID 5 0 0
5 Disabled 00:17:9a:d3:27:f5 Managed SSID 6 0 0
6 Disabled 00:17:9a:d3:27:f6 Managed SSID 7 0 0
7 Disabled 00:17:9a:d3:27:f7 Managed SSID 8 0 0
Refresh

図 7-11 「Managed Access Point Status」ページの「VAP」タブ

表 7-10 に「Managed Access Point Status」ページの「VAP」タブ内の各項目について説明します。

表 7-10 「Managed Access Point Status」ページ「VAP」タブ

項目	説明
MAC Address-Location (プルダウンメニュー)	アクセスポイントの MAC アドレスと場所。プルダウンメニューから選択したアクセスポイントの詳細情報が表示されます。
Radio （例 : 1-802.11g）	無線インタフェースと設定された無線モード。無線インタフェースを選択すると、その無線インタフェースにおいて RF スキャンによって検出された隣接クライアントを表示します。
VAP ID	VAP を識別する ID 番号（0~7）。CLI または SNMP 経由の VAP 設定に対して VAP を識別するために使用します。
VAP Mode	VAP の有効または無効を表示します。VAP の設定後、有効にした VAP のみが、ビーコンの送信やクライアントと接続することができます。
BSSID	VAP のイーサネットアドレス。
SSID	VAP に割り当てたネットワーク。各 VAP のネットワークは AP プロファイル内で設定され、SSID はネットワークコンフィグレーションに基づいています。
Client Associations	VAP に現在接続中のクライアントの総数。
Client Authentications	現在 VAP の認証を受けているクライアントの総数。

管理対象アクセスポイントの統計情報の参照

管理対象アクセスポイントの統計情報からは、アクセスポイント上の有線・無線インタフェースのトラフィックの情報が確認できます。本情報をスループットの問題などネットワークのトラブルの診断に役立てることができます。

WLAN タブ > Monitoring > Access Point > Managed Access Points とクリックし、「Statistics」タブをクリックします。

図 7-6 は 3 台のアクセスポイントについての統計情報を表示している「Managed Access Point Statistics」画面です。

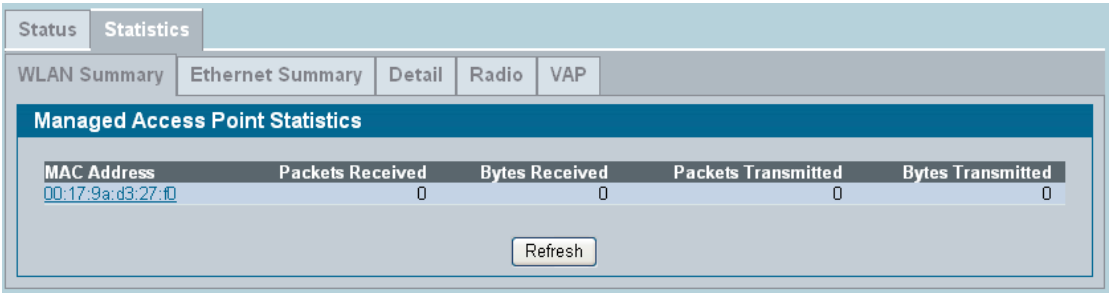


図 7-12　Managed Access Point Statistics 画面

「Managed Access Point Statistics」ページには以下のタブが利用できます。

項目	説明
WLAN Summary	スイッチが管理する各アクセスポイント上の無線インタフェースについてのサマリ情報を表示します。スイッチが管理する各アクセスポイント上の無線インタフェースについてのサマリ情報を表示します。
Ethernet Summary	スイッチが管理する各アクセスポイント上のイーサネット（有線）インタフェースについてのサマリ情報を表示します。
Detail	指定するアクセスポイントが送受信したパケット数と種類を表示します。
Radio	アクセスポイントが送受信したパケット数と種類を無線インタフェースごとに表示します。
VAP	アクセスポイントが送受信したパケット数と種類、および接続に失敗したクライアントの数を VAP ごとに表示します。

「WLAN Summary」タブや「Ethernet Summary」タブで、MAC アドレスをクリックすると、そのアクセスポイントの詳細な統計情報が確認できます。

表 7-11　「Managed Access Point Statistics」ページの「WLAN Summary」タブ

項目	説明
MAC Address	統合スイッチが管理するアクセスポイントの MAC アドレス。
Packets Received	無線ネットワーク上でアクセスポイントが受信した総パケット数。
Bytes Received	無線ネットワーク上でアクセスポイントが受信した総データ量。単位はバイトです。
Packets Transmitted	無線ネットワーク上でアクセスポイントが送信した総パケット数。
Bytes Transmitted	無線ネットワーク上でアクセスポイントが送信した総データ量。単位はバイトです。

注意 リスト中のエントリの順番を、欄の項目ごとに並び替えることができます。例えば、送信パケット数の順番でアクセスポイントを並び替える場合は、「Packets Transmitted」をクリックします。

管理対象アクセスポイントのイーサネット統計情報の参照

「Ethernet Summary」タブでは、スイッチの管理下にあるアクセスポイントの有線（イーサネット）インタフェースが送受信したパケット数およびデータ量を表示します。有線インタフェースは LAN と物理的に接続しています。

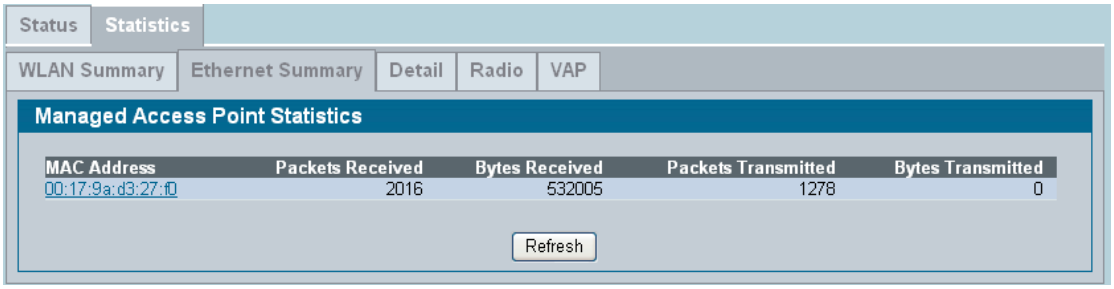


図 7-13　Managed Access Point Statistics 画面 -「Ethernet Summary」タブ

表 7-12 は「Managed Access Point Statistics」ページの「Ethernet Summary」タブ内の項目の情報を示します。

表 7-12　「Managed Access Point Statistics」ページの「Ethernet Summary」タブ

項目	説明
MAC Address	統合スイッチが管理するイーサネットの MAC アドレス。
Packets Received	有線ネットワーク上でアクセスポイントが受信した総パケット数。
Bytes Received	有線ネットワーク上でアクセスポイントが受信した総データ量。単位はバイトです。
Packets Transmitted	有線ネットワーク上でアクセスポイントが送信した総パケット数。
Bytes Transmitted	有線ネットワーク上でアクセスポイントが送信した総データ量。単位はバイトです。

管理対象アクセスポイントの統計詳細情報の参照

「Detail」タブでは、スイッチの管理下の指定したアクセスポイントの無線・有線インタフェースで送受信したパケットの数とデータ量を表示します。

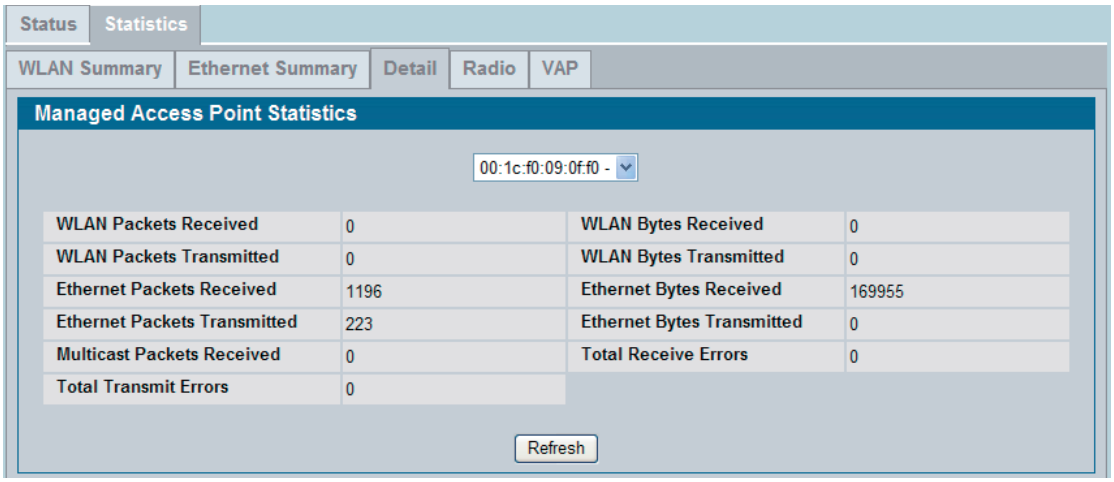


図 7-14　Managed Access Point Statistics 画面 -「Detail」タブ

表 7-13 は「Managed Access Point Statistics」ページの「Detail」タブ内の各項目の情報を示します。

表 7-13　「Managed Access Point Statistics」ページの「Detail」タブ

項目	説明
MAC Address-Location (プルダウンメニュー)	アクセスポイントの MAC アドレスと場所。プルダウンメニューから選択したアクセスポイントの詳細情報が表示されます。
WLAN Packets Received	無線ネットワーク上でアクセスポイントが受信した総パケット数。
WLAN Bytes Received	無線ネットワーク上でアクセスポイントが受信した総データ量。単位はバイトです。
WLAN Packets Transmitted	無線ネットワーク上でアクセスポイントが送信した総パケット数。
WLAN Bytes Transmitted	無線ネットワーク上でアクセスポイントが送信した総データ量。単位はバイトです。
Ethernet Packets Received	有線ネットワーク上でアクセスポイントが受信した総パケット数。
Ethernet Bytes Received	有線ネットワーク上でアクセスポイントが受信した総データ量。単位はバイトです。
Ethernet Packets Transmitted	有線ネットワーク上でアクセスポイントが送信した総パケット数。
Ethernet Bytes Transmitted	有線ネットワーク上でアクセスポイントが送信した総データ量。単位はバイトです。
Multicast Packets Received	有線ネットワーク上でアクセスポイントが受信したマルチキャストパケット数
Total Receive Errors	有線ネットワーク上で検知した受信エラーの数。
Total Transmit Errors	有線ネットワーク上で検知した送信エラーの数。

管理対象アクセスポイントの無線統計情報の参照

「Radio」タブでは、スイッチの管理下の指定アクセスポイントについて、無線インタフェースの送受信パケット数、内容などの詳細情報を参照できます。

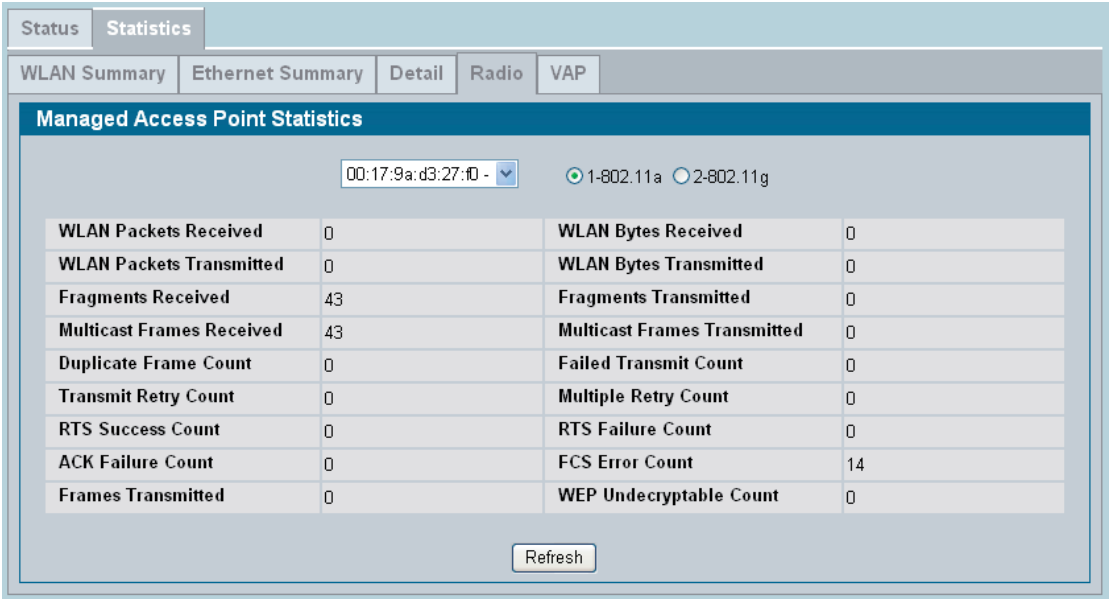


図 7-15　Managed Access Point Statistics 画面 -「Radio」タブ

表 7-14 は「Managed Access Point Statistics」ページの「Radio」タブ内の項目の情報を示します。

表 7-14　「Managed Access Point Statistics」ページの「Radio」タブ

項目	説明
MAC Address-Location (プルダウンメニュー)	アクセスポイントの MAC アドレスと場所。プルダウンメニューから選択したアクセスポイントの詳細情報が表示されます。
WLAN Packets Received	無線ネットワーク上でアクセスポイントが受信した総パケット数。
WLAN Bytes Received	無線ネットワーク上でアクセスポイントが受信した総データ量。単位はバイトです。
WLAN Packets Transmitted	無線ネットワーク上でアクセスポイントが送信した総パケット数。
WLAN Bytes Transmitted	無線ネットワーク上でアクセスポイントが送信した総データ量。単位はバイトです。
Fragments Received	正しく受信したタイプがデータまたは管理の MPDU フレーム数。
Fragments Transmitted	送信したタイプがデータまたは管理で、個別アドレスまたはマルチキャストアドレスを含む MPDU フレーム数。
Multicast Frames Received	受信した宛先 MAC アドレス中にマルチキャストビットが設定されている MSDU フレーム数。
Multicast Frames Transmitted	正しく送信した宛先 MAC アドレス中にマルチキャストビットが設定されている MSDU 数。
Duplicate Frame Count	シーケンス制御欄で duplicate（冗長）と示されているフレームを受信した回数。
Failed Transmit Count	Short retry limit/Long retry limit 超過により、MSDU が正しく送信されなかった回数。
Transmit Retry Count	1 度以上のリトライ後に MSDU が正しく送信された回数。
Multiple Retry Count	2 度以上のリトライ後に MSDU が正しく送信された回数。
RTS Success Count	RTS フレームの応答として受信された CTS フレームの数。
RTS Failure Count	RTS フレームの応答として受信されなかった CTS フレームの数。
ACK Failure Count	想定していた ACK フレームが受信されなった数。
FCS Error Count	受信した MPDU により検知した FCS エラー数。
Frames Transmitted	送信に成功した MSDU の数。
WEP Undecryptable Count	暗号化されたフレームのうち、暗号化の必要なしと示されているもの、または受信デバイスがプライバシーオプションを使用していないために廃棄されたフレームの数。

管理対象アクセスポイントの VAP 統計情報の参照

「VAP」タブでは、アクセスポイント上の指定インタフェースに定義されている VAP へのクライアントの接続・認証の失敗や、各 VAP が送受信したパケット数やデータ量の統計情報を参照できます。

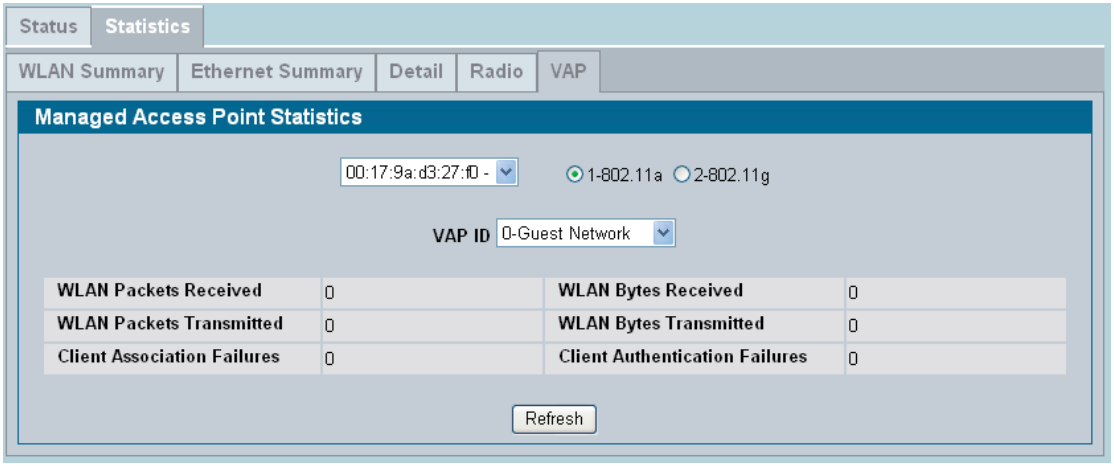


図 7-16　Managed Access Point Statistics 画面 -「VAP」タブ

表 7-15 は「Managed Access Point Statistics」ページの「VAP」タブ内の各項目の情報を示します。

表 7-15　「Managed Access Point Statistics」ページの「VAP」タブ

項目	説明
MAC Address-Location (プルダウンメニュー)	アクセスポイントの MAC アドレスと場所。プルダウンメニューから選択したアクセスポイントの詳細情報が表示されます。
Radio （例 : 1-802.11g）	無線インタフェースと設定された無線モード。無線インタフェースを選択すると、その無線インタフェースにおける VAP 統計情報を表示します。
VAP ID	プルダウンメニューで 8 つの VAP から 1 つを選択します。VAP の状態（有効 / 無効）にかかわらず選択できます。
WLAN Packets Received	指定した VAP が受信した総パケット数。
WLAN Bytes Received	指定した VAP が受信した総データ量。単位はバイト。
WLAN Packets Transmitted	指定した VAP が送信した総パケット数。
WLAN Bytes Transmitted	指定した VAP が送信した総データ量。単位はバイト。
Client Association Failures	VAP により接続を拒否されたクライアント数。
Client Authentication Failures	VAP への認証に失敗したクライアント数。

7.5 アクセスポイントの認証失敗状況の参照

アクセスポイントからスイッチへの接続は、不正なパケットフォーマットやベンダ ID などによるエラーのため、またはローカル /RADIUS データベースに Valid AP としての正しい認証情報が設定されていないなどの原因で失敗することがあります。

アクセスポイントの情報は、接続に失敗したタイミングで、接続に失敗したアクセスポイントのリストに追加され、時間が経過すると削除されます。リスト中の「Age」には、リストに追加されてからの経過時間が表示されます。**WLAN タブ > Administration > Advanced Configuration** をクリックして「Global」ページを開いて、リストから削除するタイミング（Age out）を指定することができます。また、手動でエントリを削除することも可能です。

D-Link 統合スイッチとの接続に失敗したアクセスポイントのリストを表示するためには、**WLAN タブ > Monitoring > Access Point > Authentication Failed Access Point** とクリックします。

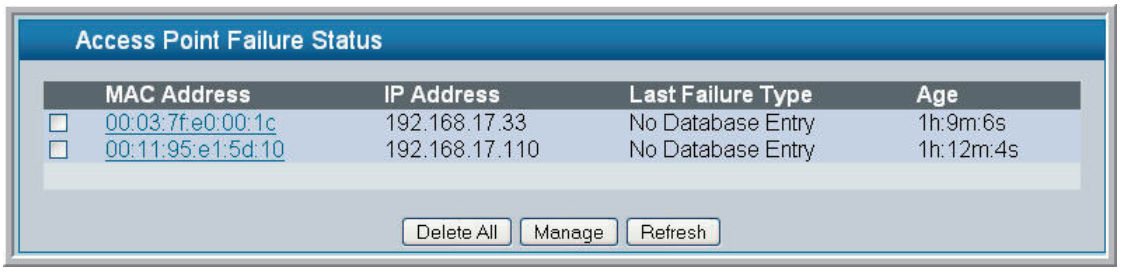


図 7-17　認証失敗のアクセスポイントの状況

「Access Point Failure Status」には、統合スイッチとのリンク確立に失敗したアクセスポイントの情報が表示されます。アクセスポイントは以下のいずれかの原因により通信に失敗します。

- No Database Entry - アクセスポイントの MAC アドレスがローカル / RADIUS サーバの Valid AP データベース中に登録されていないため、アクセスポイントの認可ができません。
- Authentication - AP に設定されている認証用パスワードがローカル / RADIUS サーバ内データベース中に登録されているものと一致しません。

リストからすべてのアクセスポイントのエントリを削除するためには「Delete All」ボタンをクリックします。本リストから、Valid AP データベースへエントリを登録するためには、MAC アドレスの左のチェックボックスを選択して、「Manage」ボタンをクリックしてください。アクセスポイントの認可をデフォルトのデータベースを使用して行っている場合は、「Administration」の下の「Basic Setup」をクリックし、「Valid AP」タブを表示し、アクセスポイントの設定を変更することができます。
アクセスポイントの認可を RADIUS サーバデータベースを使用して行っている場合は、RADIUS サーバデータベースにアクセスポイントの MAC アドレスを登録する必要があります。

不正アクセスポイントの次回検出時に、スイッチが管理する認証に失敗した AP を設定するため、MAC アドレスの左のチェックボックスを選択し、「Manage」ボタンをクリックします。「Valid Access Point Configuration」ページに表示されます。ローカルの Valid AP データベースに AP を保存するためには、AP を設定し、「Submit」ボタンをクリックします。

リスト中の MAC アドレスをクリックすることにより、そのアクセスポイントの詳しい情報を参照できます。ただし、D-Link アクセスポイント以外の場合は、いくつか参照できない値があります。

リスト中のアクセスポイントについてのビーコン情報など、さらに詳細なデータが必要な場合は「Rogue/RF Scan Access Points」ページで MAC アドレスを使用して検索してください。ただし、スイッチに有線ネットワークで接続を試みているアクセスポイントについては、RF スキャン中の検出ができない場合があります。

表 7-16　アクセスポイント認証失敗状況

項目	説明
MAC Address	アクセスポイントの MAC アドレス。
IP Address	アクセスポイントのネットワーク IP アドレス。
Last Failure Type	前回の認証失敗の原因。
Vendor ID	アクセスポイントのソフトウェアベンダ。
Validation Failures	本アクセスポイントが接続（認可）に失敗した回数。
Authentication Failures	本アクセスポイントが認証に失敗した回数。
Protocol Version	アクセスポイント上のソフトウェアがサポートするプロトコルのバージョン。
Software Version	アクセスポイント上のソフトウェアのバージョン。
Hardware Type	アクセスポイントのハードウェアプラットホーム。
Age	失敗発生からの経過時間。

7.6 不正アクセスポイントのモニタとアクセスポイントの RF スキャン

D-Link アクセスポイントの無線インタフェースでは、定期的に無線通信範囲内をスキャンすることにより、他のアクセスポイントやクライアントの情報を収集しています。アクセスポイントの通常の動作モードでは常に使用可能なチャンネルのスキャンをしています。D-Link アクセスポイントでは、通常の動作モードの他に、以下の 2 種類のスキャンモードを用意しています。

- Scan Other Channels - 定期的に使用可能なチャンネルを離れて、無線帯域内の他のチャンネルのスキャンも行います。
- Scan Sentry - 通常の無線動作を無効にし、無線スキャンを継続的に行います。本モードのアクセスポイントではビーコン送信は無効になり、クライアントからの接続も拒否します。

「Scan Other Channels」または「Scan Sentry」モードでは、アクセスポイントは無線インタフェースのすべてのチャンネルについてスキャンします。スキャンが完了すると、アクセスポイントは収集した情報を、自分を管理しているスイッチに送信します。スキャンモードの設定方法については57 ページの「5.3 無線電波の設定」を参照してください。

D-Link 統合スイッチは、RF スキャン中に検出されたアクセスポイントの MAC アドレスがローカル /RADIUSValid AP データベースに登録されていない場合、またはそのアクセスポイントがピアスイッチの管理下にない場合、それをローグ（不正）アクセスポイントと見なします。

RF スキャンによって検出されたすべてのアクセスポイント（不正と報告されたものも含む）の情報を確認することができます。
WLAN タブ > Monitoring > Access Point > Rogue/RF Scan Access Points の順にメニューをクリックし、以下の画面を表示します。

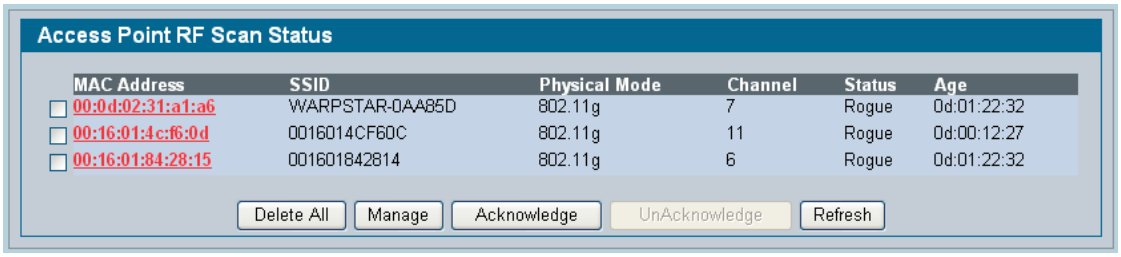


図 7-18　Access Point RF Scan Status 画面

リスト中のエントリの順番を、欄の項目ごとに並び替えることができます。例えば、不正と報告されたアクセスポイントのグループを集めたい場合は「Status」をクリックします。

アクセスポイントの情報は、検出されたタイミングで RF スキャンリストに追加され、時間が経過すると削除されます。リストの「Age」には、リストに追加されてからの経過時間が表示されます。**WLAN タブ > Administration > Advanced Configuration** をクリックして「Global」ページを開き、リストから削除するタイミング（Age out）を指定できます。また、手動で全エントリを削除するためには「Delete All」ボタンをクリックします。

不正アクセスポイントの次回検出時に、スイッチにより管理されるためには、MAC アドレスの左のチェックボックスを選択し、「Manage」ボタンをクリックします。「Valid Access Point Configuration」ページに表示されます。ローカルの Valid AP データベースに AP を保存するためには、AP を設定し、「Submit」ボタンをクリックします。
スイッチはそのアクセスポイントを Valid AP データベースに追加し、デフォルト AP プロファイルを適用します。その後スイッチからアクセスポイントを設定することができます。アクセスポイントの認知に RADIUS サーバを使用している場合は、アクセスポイントの MAC アドレスを RADIUS サーバの AP データベースに登録する必要があります。詳細については、141 ページの「付録 B 外部 RADIUS サーバの設定」を参照してください。

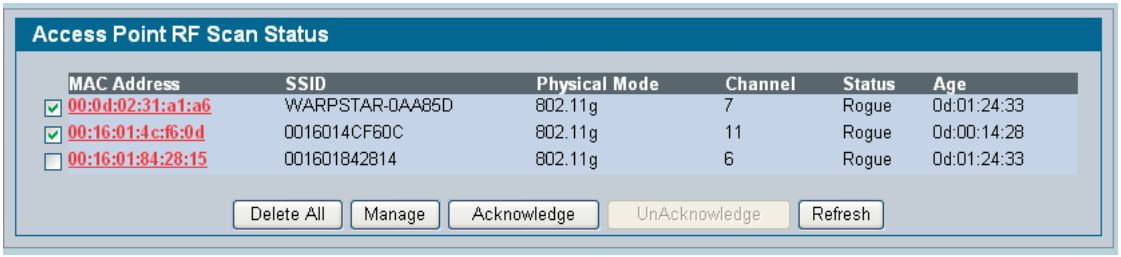


図 7-19　RF スキャン

アクセスポイントを認識済みのローグ（不正）として定義するためには、MAC アドレスの左のチェックボックスを選択し、「Acknowledge」ボタンをクリックします。スイッチはそのアクセスポイントを認識済みローグ（不正）として Valid AP データベースに追加します。
不正アクセスポイントを管理または認識する場合、スイッチは Valid AP データベースにそのエントリを追加しますが「RF Scan Status」リストの内容は変更されません。しかし、次回そのアクセスポイントが検出された場合、「Access Point RF Scan Status」リストの内容は更新されて表示されます。

アクセスポイントをローグ（不正）として定義するためには、認識済みの AP の MAC アドレス左のチェックボックスを選択し、「UnAcknowledge」ボタンをクリックします。Valid AP データベースから AP を削除します。

検出されたアクセスポイントについての詳細情報を確認するためには、そのエントリの「MAC Address」のリンクをクリックしてください。

詳細情報には、「Access Point RF Scan Status」ページの情報の他に、送信速度などのビーコンフレームより取得した情報が含まれます。

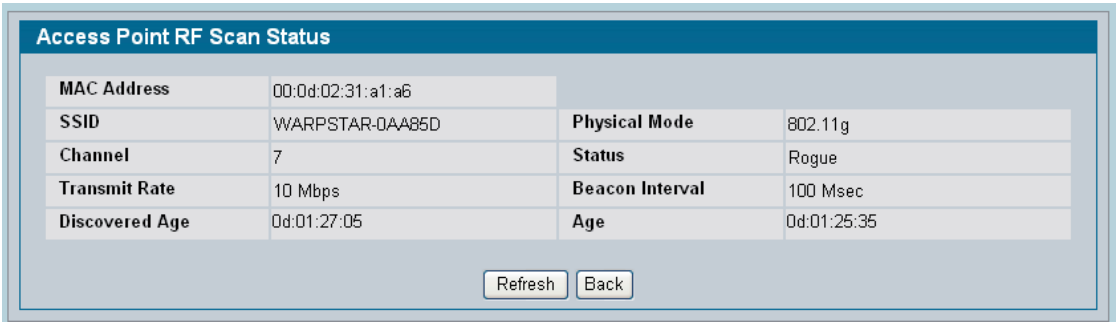


図 7-20　Access Point RF Scan Status 画面

以下の表に「Access Point RF Scan Status」ページから確認できる情報を示します。

表 7-17 「Access Point RF Scan Status」ページ

項目	説明
MAC Address	検出されたアクセスポイントの MAC アドレスで物理的な無線インタフェースまたは VAP の MAC アドレス。D-Link アクセスポイントの場合は常に VAP の MAC アドレスです。
SSID	ネットワークの SSID。ブロードキャストされたビーコンフレームから検出します。
Physical Mode	アクセスポイントで使用している 802.11 のモードを示します。
Channel	アクセスポイントの通信チャンネル。
Status	アクセスポイントの管理状況を示します。スイッチに認識されている有効なアクセスポイントであるか、またはローグ（不正）と見なされているかなどの情報を取得できます。以下の情報の一つが表示されます。 • WS Managed - 本アクセスポイントは、本スイッチの管理下にあります。アクセスポイントの状態は MAC アドレスにより参照できます。 • Peer WS Managed - 本アクセスポイントは、同一ピアグループ内の他のスイッチにより管理されています。 • Acknowledged Rogue - 本アクセスポイントは、Valid AP エントリとしてローカルまたは RADIUS サーバに登録されています。認証され、不正アクセスポイントとの報告はされていません。 • Ad Hoc Rogue - 本アクセスポイントはアドホックネットワークに参加していることが検知されました。
Transmit Rate	アクセスポイントの現在の送信速度。
Beacon Interval	隣接アクセスポイントネットワークへのビーコン間隔。
Discovered Age	本アクセスポイントが最初に RF スキャンで検出されてからの経過時間。単位は秒。
Age	本アクセスポイントが最後に RF スキャンで検出されてからの経過時間。単位は秒。

7.7 接続中のクライアントのモニタ

スイッチ管理対象のアクセスポイントが接続中の無線クライアントについて、さまざまな情報を参照することができます。

接続中のクライアントの情報にアクセスするためには、**WLAN タブ > Monitoring > Client > Associated Clients** の順にメニューをクリックします。

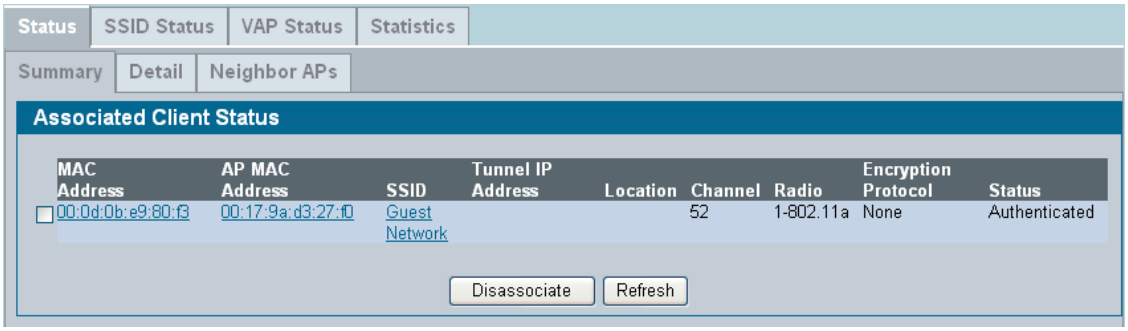


図 7-21 「Associated Client Status」ページ

本ページでは以下のタブが利用可能です。

項目	説明
Status	スイッチ管理対象のアクセスポイントと接続中のクライアントの状態。以下の情報が表示されます。 - Summary - 接続中のクライアントの基本的な情報。 - Detail - 接続中のクライアントの詳細情報（例 : クライアントが接続している VLAN。クライアントが非アクティブである時間など）。 - Neighbor APs - クライアントの通信範囲内にある管理対象のアクセスポイントを表示します。接続中のクライアントがローミングに使用するアクセスポイントを決定する場合に役立てることができます。
SSID Status	SSID と、そのネットワークに接続するクライアントの MAC アドレス。
VAP Status	D-Link アクセスポイント上の指定した VAP に接続中のクライアントを表示します。
Statistics	アクセスポイントに接続中のクライアントについて、以下の統計情報を表示します。 - Association Summary - 1 台のアクセスポイントと接続中のクライアントの統計情報。 - Session Summary - クライアントが、異なるアクセスポイント間でローミングする際のセッション全体についての統計情報。 - Association Detail - 1 台のアクセスポイントと接続中のクライアントが送受信するパケットの詳細情報。 - Session Detail - 1 台、またはローミング時には複数のアクセスポイントと接続中のクライアントが送受信するパケットの詳細情報。

接続クライアントデータベースがアクセスポイント間のローミングをサポートするため、クライアントがあるアクセスポイントと接続を終了しても、エントリは削除されません。接続終了後のエントリは、タイムアウト時間後に削除されます。このタイムアウト時間は、**WLAN タブ > Administration > Advanced Configuration** をクリックして表示できる「Global」ページ中の「Client Roam Timeout」欄で設定できます。このタイムアウト時間はクライアントが他のアクセスポイントにローミングするために与えられた時間と一致します。

接続中のクライアントの状態の参照

表 7-18 には「Associated Client Status」ページの「Summary」タブ内の各項目の情報を表示します。

表 7-18 「Associated Client Status」ページの「Summary」タブ

項目	説明
MAC Address	クライアントの MAC アドレス。
AP MAC Address	クライアントが接続中のアクセスポイントの MAC アドレス。
SSID	クライアントが接続中のネットワークを表示します。
Tunnel IP Address	クライアントが L3 トンネルを使用している場合、クライアントの IP アドレスが表示されます。使用していない場合は表示はありません。
Location	クライアントが接続中のアクセスポイントの場所。アクセスポイントの場所は Valid AP データベースに設定されています。
Channel	クライアントの接続に使用されているチャンネル。
Radio	クライアントが使用している無線モード。
Encryption Protocol	クライアントが WLAN 接続のために使用する暗号化プロトコル。
Status	クライアントが接続中であるか、認証されているかを示しています。以下のいずれかが表示されます。 • Associated - クライアントは現在管理対象のアクセスポイントと接続中です。 • Authenticated - クライアントは現在接続中で、アクセスポイントに認証されています。 • Disassociated - クライアントはアクセスポイントと接続していません。タイムアウト時間内に他の管理対象アクセスポイントとローミングを開始しない場合は削除されます。

接続中のクライアントの詳細情報の参照

スイッチの管理下にあるアクセスポイントと接続中の各クライアントについて、詳細な接続状況を確認することができます。

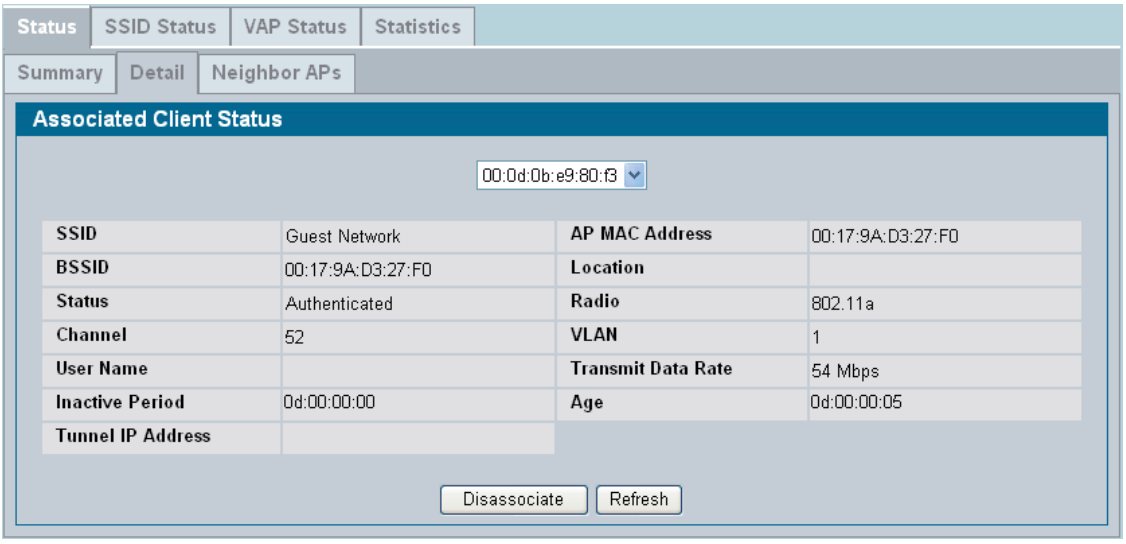


図 7-22 「Associated Client Status」-「Detail」タブ

表 7-19 には「Associated Client Status」ページの「Detail」タブ内の各項目の情報を示します。

表 7-19 「Associated Client Status」ページの「Detail」タブ

項目	説明
MAC Address	クライアントの MAC アドレス。プルダウンメニューから MAC アドレスを選択すると、そのクライアントについての詳細情報が表示されます。
SSID	クライアントが接続中のネットワークを表示します。
AP MAC Address	クライアントが接続中のアクセスポイントの MAC アドレス。
BSSID	クライアントが接続中のアクセスポイントの VAP の MAC アドレス。
Location	クライアントが接続中のアクセスポイントの場所。
Status	クライアントが接続中であるか、認証されているかを示しています。以下の一つが表示されます。 • Associated - クライアントは現在管理対象のアクセスポイントと接続中です。 • Authenticated - クライアントは現在接続中で、アクセスポイントに認証されています。 • Disassociated - クライアントはアクセスポイントと接続していません。タイムアウト時間内に他の管理対象アクセスポイントとローミングを開始しない場合は削除されます。
Radio	クライアントの接続に使用されている無線インタフェース。
Channel	クライアントの接続に使用されているチャンネル。
VLAN	クライアントが VAP と接続中で VLAN データ送信モードである時、現在割り当てられている VLAN を表示します。
User Name	802.1X により認証されているクライアントのユーザ名。他のセキュリティモードを使用しているクライアントはユーザ名の表示はありません。
Transmit Data Rate	クライアントの現在のデータ送信速度。
Inactive Period	現在の接続でアクセスポイントがクライアントからのトラフィックを検出していない時間。
Age	スイッチがクライアントから新規に接続データを受信してからの経過時間。単位は秒です。
Tunnel IP Address	クライアントがトンネルを使用している場合、割り当てられたトンネル IP アドレスが表示されます。トンネルを使用しないクライアントの場合、何も表示されません。
Captive Portal	無線クライアントがキャプティブポータル経由でネットワークにアクセスし、スイッチに認証された場合にだけ、本欄は表示されます。 クライアントのキャプティブポータル接続に関する追加情報を参照するためには、「Authenticated」ボタンをクリックし、**Captive Portal > Client Connection Status** ページからアクセス可能な詳細なクライアント情報にリンクします。

接続中のクライアントの隣接アクセスポイントの状態の参照

「Associated Client Status」ページの「Neighbor APs」タブでは、接続中のクライアントが検知したアクセスポイントの情報を参照することができます。本ページに表示する情報は、接続中のクライアントがローミングするために使用するアクセスポイントを決定する際に役立てることができます。

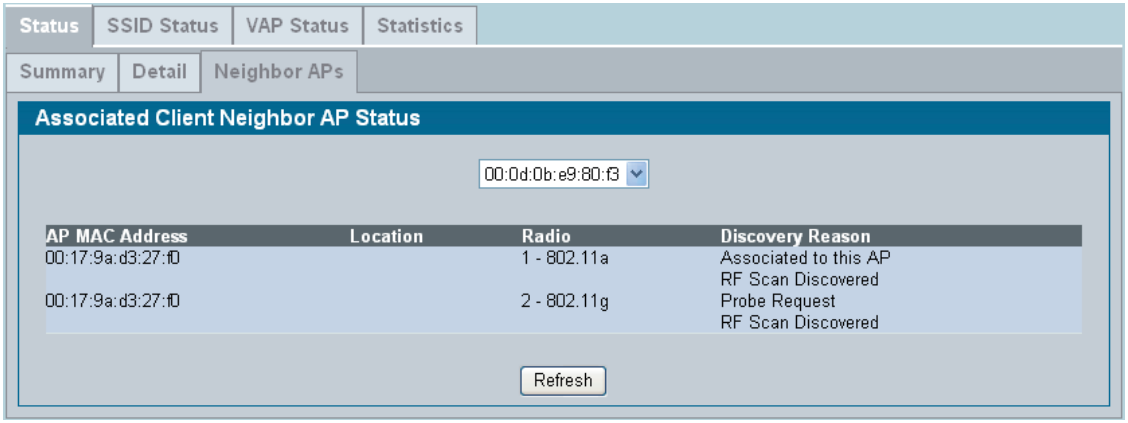


図 7-23 「Associated Client Status」-「Neighbor APs」タブ

表 7-20 には「Associated Client Status」ページの「Neighbor APs」タブ内の各項目の情報を示します。

表 7-20 「Associated Client Status」ページの「Neighbor APs」タブ

項目	説明
MAC Address	クライアントの MAC アドレス。プルダウンメニューから MAC アドレスを選択すると、そのクライアントについての詳細情報が表示されます。
AP MAC Address	統合スイッチ管理下のアクセスポイントの MAC アドレス。
Location	アクセスポイントの場所。
Radio	本クライアントを隣接クライアントとして検出した無線インタフェースと無線モード。
Discovery Reason	隣接クライアントの検出原因。複数の原因が表示される場合があります。 • RF Scan - 本隣接クライアントは、RF スキャンにより報告されました。RF スキャンによるクライアント検出は困難なため、通常は本原因以外が表示されます。 • Probe Request - 管理対象のアクセスポイントが本隣接クライアントからプローブリクエストを受信しました。 • Associated to Managed AP - 本隣接クライアントは、当スイッチ管理下の他のアクセスポイントと接続しています。 • Associated to This AP - 本隣接クライアントは、当アクセスポイントと接続しています。 • Associated to Peer AP - 本隣接クライアントは、ピアスイッチの管理下のアクセスポイントと接続しています。 • Ad Hoc Rogue - 本隣接クライアントはアドホックネットワークに参加していることが検知されました。

接続中のクライアントの SSID の参照

各アクセスポイントは、それぞれ異なる SSID を持つ 16 個までのネットワークを持つことができます。複数のクライアントが同一の物理アクセスポイントに接続していても、同じ SSID を使用して接続していない場合もあります。

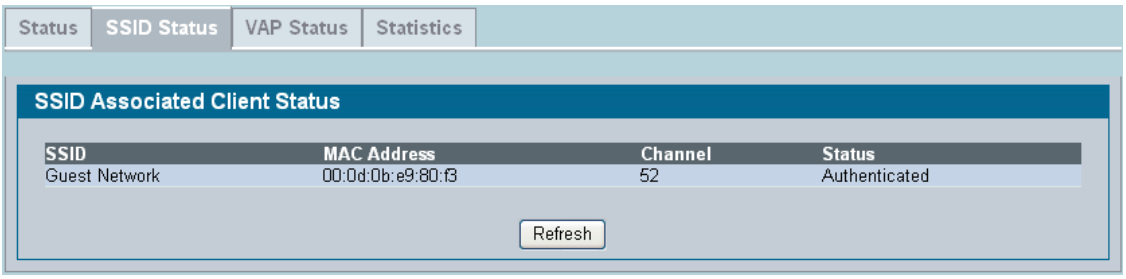


図 7-24 「Associated Client Status」-「SSID Status」タブ

「SSID Status」タブでは、各クライアントが接続しているネットワークの SSID を表示します。

表 7-21 「Associated Client Status」ページの「SSID Status」タブ

項目	説明
SSID	クライアントが接続しているネットワークを示します。
MAC Address	クライアントの MAC アドレス。
Channel	クライアントの接続に使用しているチャンネル。
Status	クライアントが接続中であるか、認証されているかを示しています。以下のいずれかが表示されます。 • Associated - クライアントは現在管理対象のアクセスポイントと接続中です • Authenticated - クライアントは現在接続中で、アクセスポイントに認証されています。 • Disassociated - クライアントはアクセスポイントと接続していません。タイムアウト時間内に他の管理対象アクセスポイントとローミングを開始しない場合は削除されます。

接続中のクライアントの VAP の参照

各アクセスポイントは、各無線インタフェースに対して 8 個の仮想アクセスポイント（VAP）を持ち、各 VAP は固有の MAC アドレス（BSSID）を持ちます。「VAP Status」タブでは、クライアントと接続している VAP の情報を参照することができます。

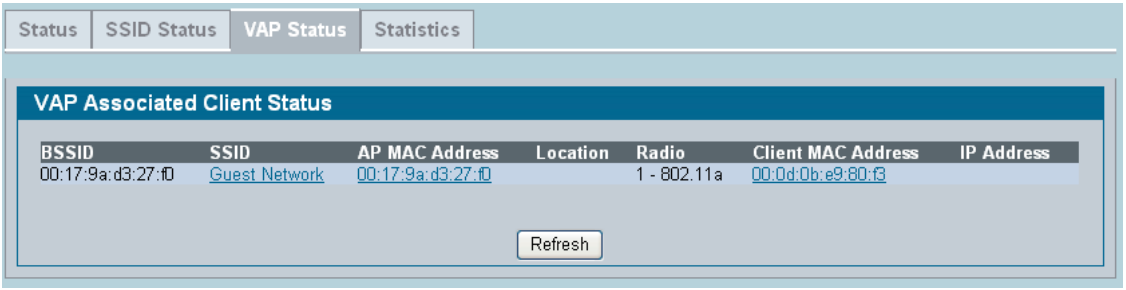


図 7-25 「Associated Client Status」-「VAP Status」タブ

表 7-22 「Associated Client Status」ページの「VAP Status」タブ

項目	説明
BSSID	本クライアントが接続中の VAP の MAC アドレス。
SSID	WLAN 接続のためにクライアントが使用している SSID。
AP MAC Address	管理対象アクセスポイントの MAC アドレス。
Location	管理対象アクセスポイントの場所。
Radio	クライアントが接続中のアクセスポイントの無線インタフェースと無線モード。
Client MAC Address	クライアントの MAC アドレス。
IP Address	VAP に接続中のクライアントの IP アドレス。

接続中のクライアントの統計情報の参照

無線クライアントは、WLAN サービスを中断せずに、アクセスポイント間をローミングすることができます。D-Link 統合スイッチは、スイッチが管理するアクセスポイントの間をクライアントがローミングをする間に送受信されるトラフィックをトレースしています。スイッチはクライアントが 1 台のアクセスポイントと接続中も、また複数台のアクセスポイント間をローミング中でも、統計情報を記録しています。

「Statistics」タブの「Association Summary」の統計情報では、1 台のアクセスポイントと通信中のクライアントが送受信したトラフィックの情報を示しています。

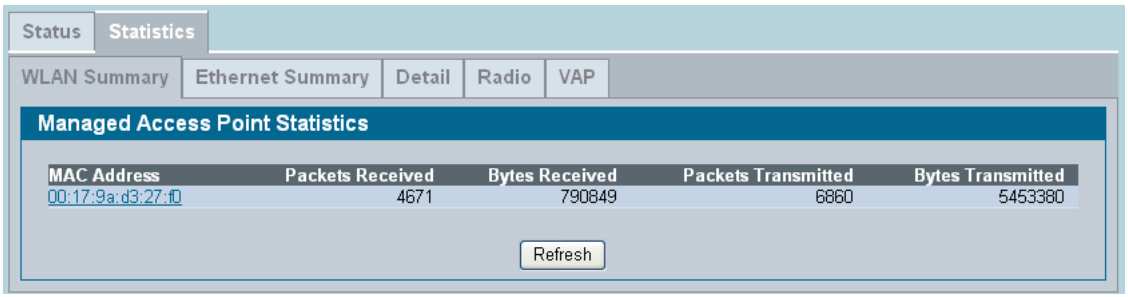


図 7-26 「Associated Client Status」-「Association Summary」タブ

表 7-23 接続中のクライアントの接続統計サマリ情報

項目	説明
MAC Address	クライアントの MAC アドレス。
Packets Received	クライアントから受信したパケット数。
Bytes Received	クライアントから受信したデータ量。単位はバイトです。
Packets Transmitted	クライアントに送信したパケット数
Bytes Transmitted	クライアントに送信したデータ量。単位はバイトです。

「Session Summary」の統計情報では、クライアントが、スイッチ管理下のアクセスポイントが共有する同一の WLAN ネットワークに接続している間に送受信するトラフィックについての情報を確認することができます。

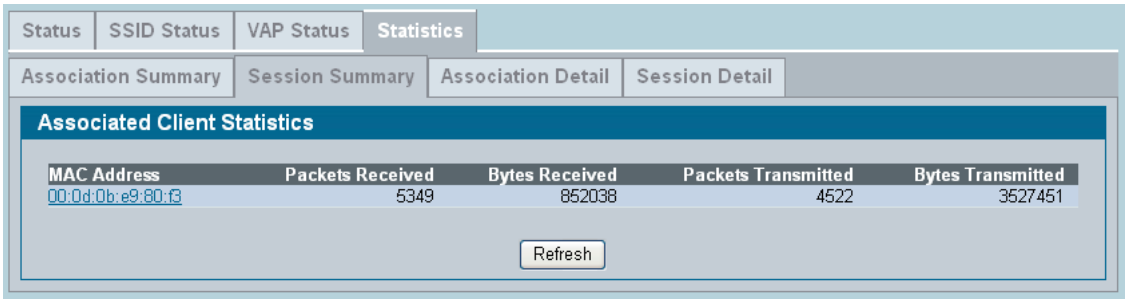


図 7-27 「Associated Client Status」-「Session Summary」タブ

あるクライアントがアクセスポイントから他のアクセスポイントへローミングする時、それが同じネットワーク内であれば、そのセッションは継続していると見なされ、セッション統計は累積されます。クライアントが無線通信を終了した場合、またはスイッチ管理下のアクセスポイントの通信範囲を出た場合、そのセッションは終了したものと見なされます。

表 7-24 通信中のクライアントのセッション統計サマリ情報

項目	説明
MAC Address	クライアントの MAC アドレス。
Packets Received	クライアントから受信した総パケット数。
Bytes Received	クライアントから受信した総データ量。単位はバイトです。
Packets Transmitted	クライアントに送信した総パケット数。
Bytes Transmitted	クライアントに送信した総データ量。単位はバイトです。

「Association Detail」の統計情報では、クライアントが 1 台のアクセスポイントに接続中に送受信したトラフィックの詳細情報を参照できます。

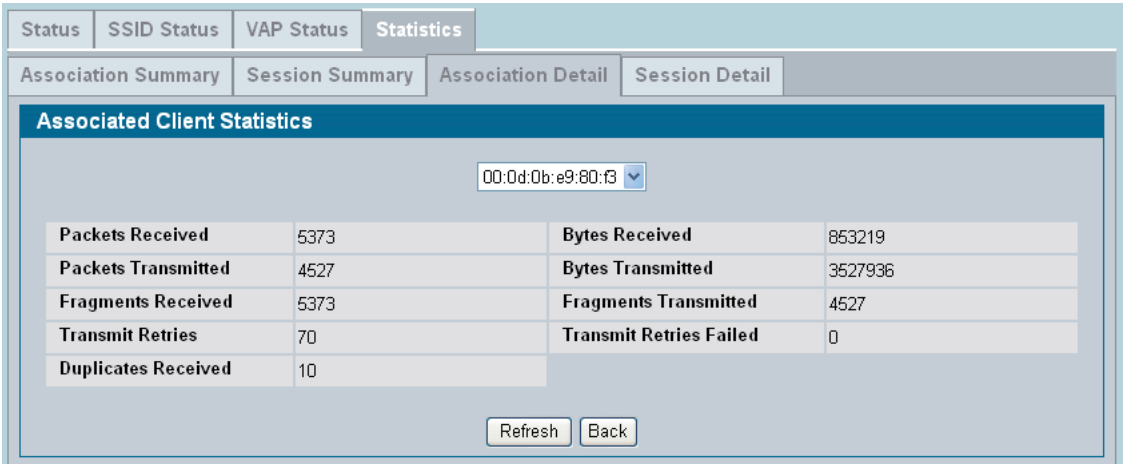


図 7-28 「Associated Client Status」-「Association Detail」タブ

表 7-25 接続中のクライアントの接続詳細統計情報

項目	説明
MAC Address（プルダウンメニュー）	クライアントの MAC アドレス。プルダウンメニューで MAC アドレスを選択し、詳細情報を表示します。
Packets Received	クライアントから受信した総パケット数。
Bytes Received	クライアントから受信した総データ量。単位はバイトです。
Packets Transmitted	クライアントに送信した総パケット数。
Bytes Transmitted	クライアントに送信した総データ量。単位はバイトです。
Fragments Received	クライアントから受信したフラグメント化されたパケット総数。
Fragments Transmitted	クライアントに送信したフラグメント化されたパケット総数。
Transmit Retries	1 回以上のリトライの後、クライアントに送信成功した回数。
Transmit Retries Failed	1 回以上のリトライの後、クライアントに送信失敗した回数。
Duplicates Received	クライアントから受信した冗長パケットの総数。

「Session Detail」の統計情報では、クライアントがスイッチ管理下のアクセスポイントが共有する同一の WLAN ネットワークに接続しているあいだに送受信するトラフィックの情報を参照することができます。

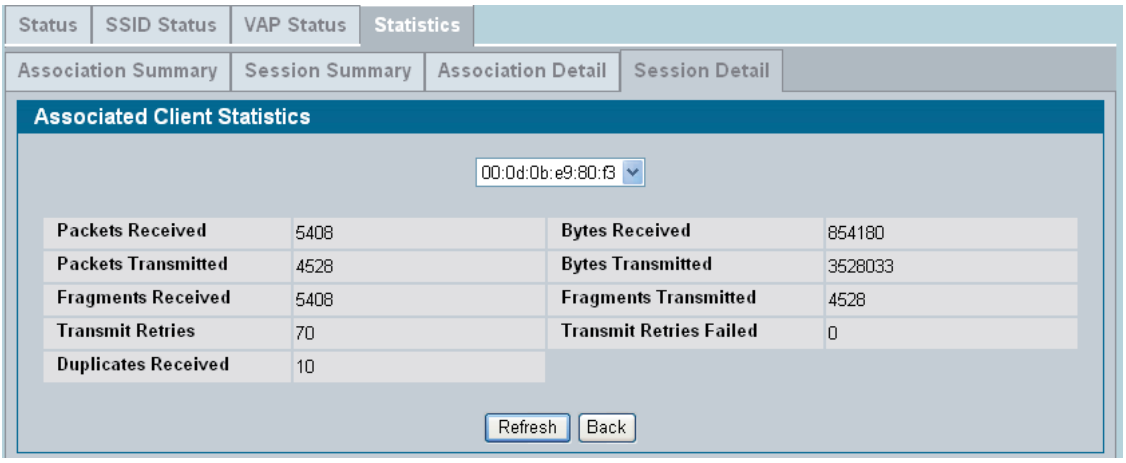


図 7-29 「Associated Client Status」-「Session Detail」タブ

表 7-26 接続中のクライアントのセッション詳細統計情報

項目	説明
MAC Address（プルダウンメニュー）	クライアントの MAC アドレス。プルダウンメニューで MAC アドレスを選択し、詳細情報を表示します。
Packets Received	クライアントから受信した総パケット数。
Bytes Received	クライアントから受信した総データ量。単位はバイトです。
Packets Transmitted	クライアントに送信した総パケット数。
Bytes Transmitted	クライアントに送信した総データ量。単位はバイトです。
Fragments Received	クライアントから受信したフラグメント化されたパケット総数。
Fragments Transmitted	クライアントに送信したフラグメント化されたパケット総数。
Transmit Retries	1 回以上のリトライの後、クライアントに送信成功した回数。
Transmit Retries Failed	1 回以上のリトライの後、クライアントに送信失敗した回数。
Duplicates Received	クライアントから受信した冗長パケットの総数。

7.8 クライアントの認証失敗状況の参照

アクセスポイントへの接続または認証に失敗した無線クライアントは、「Client Failure」リスト上に失敗した回数とともに表示されます。失敗の原因としては、クライアント側とアクセスポイント側のセキュリティまたは認証情報が一致しなかった可能性があります。

クライアントの情報は、接続に失敗したタイミングでリストに追加され、時間が経過すると削除されます。リスト中の「Age」欄には、リストに追加されてからの経過時間が表示されます。

WLAN タブ > Administration > Advanced Configuration > Global 画面でリストから削除するタイミング（Age out）を指定することができます。また、手動でエントリを削除することも可能です。

アクセスポイントへの接続または認証に失敗した無線クライアントを表示するためには「Authentication」の「Authentication Failed Clients」ページをクリックしてください。

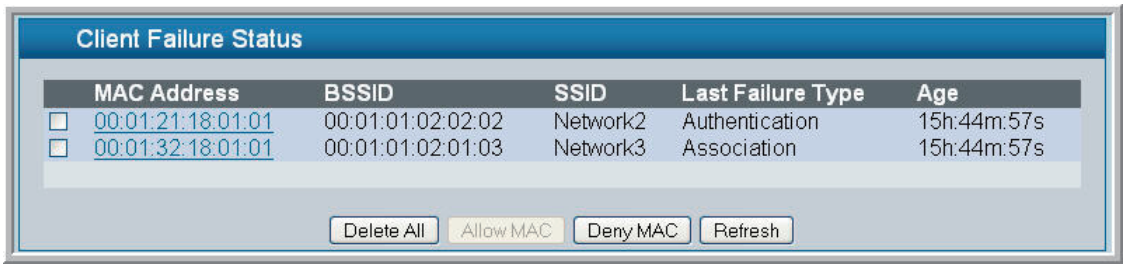


図 7-30　クライアントの認証失敗状況

リストからすべてのクライアントを削除するためには、「Delete All」ボタンをクリックします。

認証に失敗したクライアントから WLAN へのアクセスを防ぐためには、そのクライアントの MAC アドレスの左側にあるチェックボックスを選択して「Deny MAC」ボタンをクリックします。するとその MAC アドレスは、デフォルトアクションが「Deny（拒否）」である AP プロファイル用の「MAC Authentication Deny MAC」リストに追加されます。反対に、デフォルトアクションが「Allow（許可）」である AP プロファイル用の「MAC Authentication Allow MAC」リストに MAC アドレスを追加したい場合は、クライアントを選択して「Allow MAC」ボタンをクリックします。その後、変更事項をアクセスポイントに反映させるために、AP プロファイルを再適用する必要があります。

注意 「Deny MAC」ボタンがグレー表示で選択ができない場合は、すべてのプロファイルで MAC 認証動作の初期値として「Allow（許可）」が設定されていることを意味しています。同様に「Allow MAC」ボタンのグレー表示の場合は、すべてのプロファイルにおいて MAC 認証動作の初期値として「Deny（拒否）」が設定されています。

注意 AP プロファイルにおいて、MAC 認証に RADIUS サーバを使用しているものがある場合は、MAC アドレスを RADIUS サーバのデータベースに追加する必要があります。

表 7-27 は接続に失敗したクライアントのサマリ情報ページ中の各項目について説明します。

表 7-27　接続失敗クライアントの状況

項目	説明
MAC Address	クライアントの MAC アドレス。
BSSID	クライアントが接続 / 認証を試みた VAP の MAC アドレス。
SSID	クライアントが接続 / 認証を試みたネットワークの SSID。
Last Failure Type	最後に発生した失敗の種類。「Authentication（認証）」または「Association（接続）」が表示されます。
Age	失敗発生からの経過時間。

クライアントの MAC アドレスをクリックすると、そのクライアントについての追加情報を表示できます。

注意 クライアント側で間違った WEP キーが設定されていると、本ページに認証に失敗したクライアントが表示されない場合があります。これは IEEE 802.11 規格における既知の問題によるものです。この規格では、アクセスポイントが 3 番目のフレーム（暗号化されたチャレンジテキストを含む）を復号できない場合、unsuccessful result を送信することになっています。しかし、アクセスポイントが WEP フレームを復号できない場合は、そのフレームは 3 番目のフレームであったか、または共通鍵フレームであったかを判別できないため、結果の送信を行いません。これは、共通鍵認証する WEP 認証方式において、不正確なキーが登録された場合にだけ該当する問題です。

各クライアントの認証失敗の状況の表示から、認証または接続に失敗したクライアントと失敗の回数を確認することができます。認証に何度も失敗しているクライアントは、WLAN にとって危険な存在である可能性もあります。

表 7-28 には「Authentication Failed Client Status」ページの「Detail」タブの各項目について説明しています。

表 7-28 「Authentication Failed Client Status」ページの「Detail」タブ

項目	説明
MAC Address	クライアントの MAC アドレス。
BSSID	クライアントが接続 / 認証を試みた VAP の MAC アドレス。
SSID	クライアントが接続 / 認証を試みたネットワークの SSID。
Last Failure Type	最後に発生した失敗の種類。「Authentication（認証）」または「Association（接続）」が表示されます。
Authentication Failure Count	本クライアントが認証に失敗した回数。
Association Failure Count	本クライアントが接続に失敗した回数。
Age	失敗発生からの経過時間。

7.9 アドホッククライアントのモニタと管理

アドホッククライアントとは、アクセスポイントに接続しているクライアントを経由して WLAN に接続するクライアントです。アドホッククライアントは、直接アクセスポイントと通信を行いません。アドホックネットワークは、RF 帯域を消費し、セキュリティ上のリスクを招く可能性を含んでいるため、特に注意が必要です。

アドホッククライアントの情報は、検出されたタイミングで、アドホッククライアントのリストに追加され、時間が経過すると削除されます。リスト中の「Age」欄には、リストに追加されてからの経過時間が表示されます。

WLAN タブ > Administration > Advanced Configuration > Global 画面でリストから削除するタイミング（Age out）を指定することができます。また、手動でエントリを削除することも可能です。

WLAN タブ > Monitoring > Client をクリックして「Ad Hoc Clients」ページを表示し、アドホックネットワークによって WLAN に接続しているクライアントを検索し、管理します。

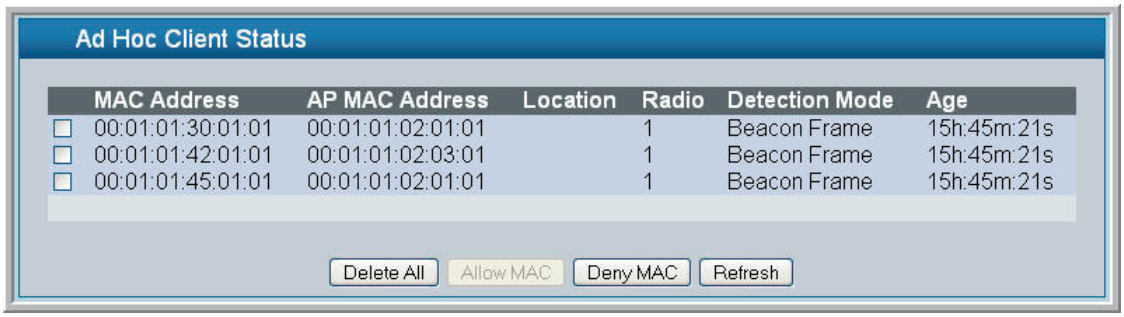


図 7-31
アドホッククライアント

リストからすべてのアドホッククライアントを削除するためには、「Delete All」ボタンをクリックします。本リストはクリアされます。

注意 リストをクリアしても、アドホッククライアントは切断されません。リスト上から削除されても、クライアントはアドホックネットワークに残っている場合があります。

アドホッククライアントから WLAN へのアクセスを防ぐためには、目的のクライアントの MAC アドレスの左側にあるチェックボックスを選択して「Deny MAC」ボタンをクリックします。するとその MAC アドレスは、AP プロファイルの MAC 認証設定の「MAC Deny」リストに追加されます。反対に、AP プロファイルの MAC 認証設定の「Allow MAC」リストに追加する場合は、クライアントを選択して「Allow MAC」ボタンをクリックします。

注意 MAC アドレスは、グローバルデフォルトアクションが「Allow（許可）」または「Deny（拒否）」である AP プロファイル用のローカル MAC 認証リストに対して追加されます。AP プロファイルにおいて、MAC 認証に RADIUS サーバを使用しているものがある場合は、MAC アドレスを RADIUS サーバのデータベースに追加する必要があります。

各 AP プロファイルは、1 つのグローバル MAC 認証リストを持っています。これは「リスト上のすべての MAC アドレスへのアクセスを拒否するもの」または「リスト上のすべての MAC アドレスへのアクセスを許可するもの」となります。デフォルト AP プロファイルに、どちらかのモードを設定するためには「Administration」>「Basic Setup」とクリックし、「AAA/RADIUS」タブを選択して「MAC Authentication」の「Default Action」欄でリスト中のすべての MAC アドレスを「Deny（拒否）」または「Allow（許可）」を設定します。特定の AP プロファイルへのモード設定は「AP Profiles」で AP プロファイル名のタブの「Global」タブ上で実行できます。

クライアントがアクセスポイントによる認証に成功した場合でも、スイッチは本リストから MAC エントリを削除することはありません。アドホックデータヒストリに記録が残るので、WLAN 上でアドホックネットワークを構成するクライアントを慎重に扱うことができます。

表 7-29　アドホッククライアントの状態

項目	説明
MAC Address	クライアントの MAC アドレス。検出モードがビーコンフレームの場合、RF スキャンデータベースや隣接 AP リストには、クライアントはアクセスポイントとして表示されます。検出モードがデータフレームの場合、クライアント情報は隣接クライアントリストに表示されます。
AP MAC Address	クライアントを検出したアクセスポイントの MAC アドレス。
Location	アクセスポイントの場所。
Radio	アドホッククライアントが検出された無線インタフェースと無線モード。
Detection Mode	アドホッククライアントの検出方式。「Beacon Frame」または「Data Frame」が表示されます。
Age	アドホックネットワークが最後に検出されてからの経過時間（秒）。

第 8 章　システムの詳細設定

本章は以下の項により構成し、D-Link 統合アクセスシステムネットワークの設定に有効な情報を提供します。

項目	説明	参照ページ
アクセスポイントプロファイルの作成、設定、管理	アクセスポイントプロファイルの作成、設定、管理を行います。	108 ページ
グローバル設定	D-Link 統合スイッチに対してグローバルな設定を行います。	111 ページ
SNMP トラップの有効化	スイッチに SNMP エージェントを設定して、ネットワーク内の SNMP マネージャにトラップ送信します。	112 ページ
QoS の設定	無線インタフェースごとに QoS の設定を行います。	113 ページ

8.1 アクセスポイントプロファイルの作成、設定、管理

アクセスポイント・コンフィグレーションプロファイルは、さまざまなユーザ層において使用されるアクセスポイントを集約する、規模の大きな無線ネットワークに非常に有効な機能です。D-Link 統合スイッチ上で多数の AP プロファイルを作成することにより、場所、機能なまたは他の要素に基づいてアクセスポイントをカスタマイズすることができます。プロファイルとはテンプレートのようなもので、作成した AP プロファイルは統合スイッチ管理下のアクセスポイントに適用することができます。

各 AP プロファイルには、以下の機能を設定することができます。

- グローバル RADIUS 設定
- MAC 認証リスト
- 無線設定
- ネットワーク設定
- QoS 設定

図 8-1 は、あるキャンパスのネットワークにおいて、D-Link 統合スイッチの管理下に 10 台のアクセスポイントがあることを示しています。各建物には複数のアクセスポイントが設置されており、ネットワークの必要条件は各建物により異なるものとします。

本 WLAN の管理者は、デフォルトプロファイルに加えて、2 つの AP プロファイルを作成しています。

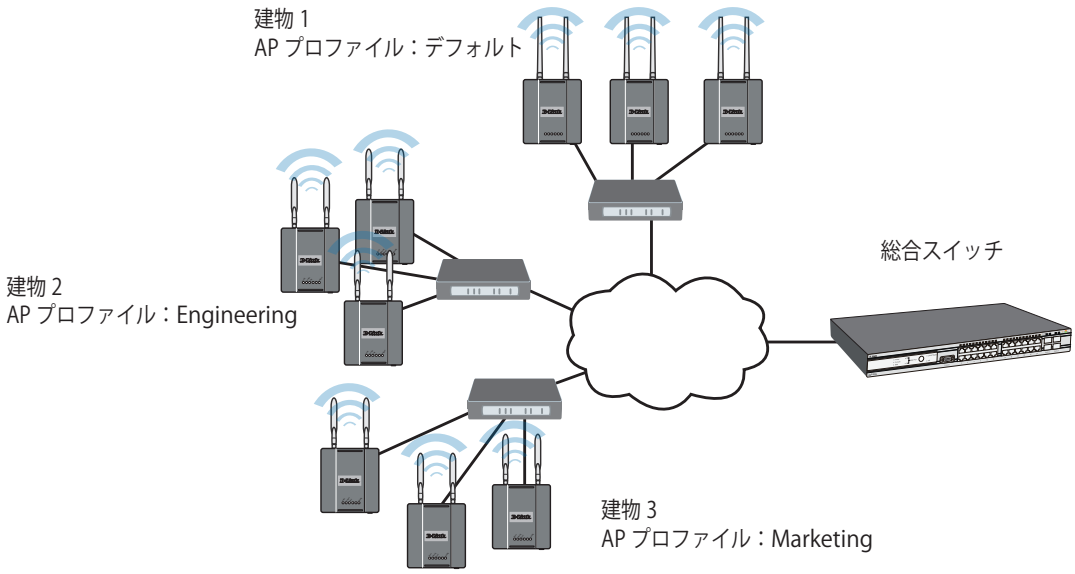


図 8-1　複数の AP プロファイル

建物 1 にはメインロビーといくつかの会議室があります。この場所の WLAN ユーザは主に職員以外の人と訪問者です。建物 1 のアクセスポイントには、デフォルト AP プロファイルを適用し、追加のネットワークおよびセキュリティの設定はしていません。

建物 2 は工学部の建物です。建物 2 のアクセスポイントには「Engineering」というプロファイルを使用しています。「Engineering」AP プロファイルには、異なる SSID（Hardware、Software、Test）を持つ 3 つの VAP が定義されています。

建物 3 はセールスとマーケティングの建物です。建物 3 のアクセスポイントには「Marketing」というプロファイルを使用しています。「Marketing」AP プロファイルには、異なる SSID（Sales、Marketing、Program Management）を持つ 3 つの VAP が定義されています。

ネットワーク管理者が建物 2 にもう 1 台のアクセスポイントを設置する場合、AP 認知プロセス中に、アクセスポイントに対して「Engineering」プロファイルが割り当てられます。

アクセスポイントプロファイルの作成、コピー、削除

「Access Point Profile Summary」ページを使用すると、AP プロファイルの作成、コピーおよび削除をすることができます。D-Link 統合スイッチでは 16 件までの AP プロファイルを作成できます。

WLAN タブ > Administration > Advanced Configuration > AP Profiles とクリックします。新しいプロファイルを作成するためには、「Profile」欄にプロファイル名を入力し、「Add」ボタンをクリックします。

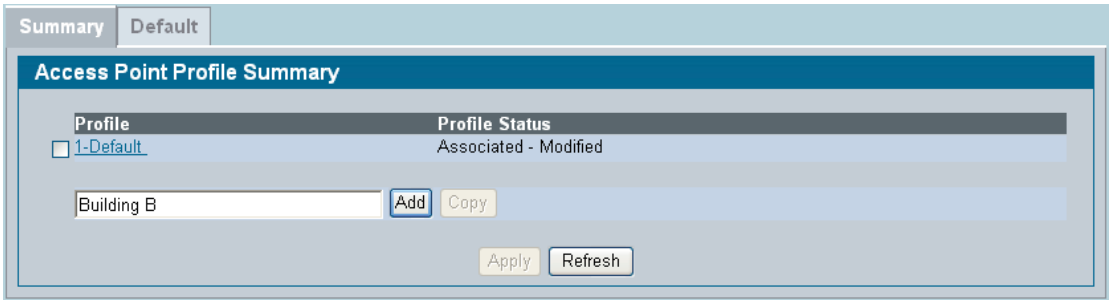


図 8-2　プロファイルの追加

プロファイルを追加すると、そのプロファイル用にプロファイル設定ページが表示され、そのページの上部に、作成したプロファイル名のタブが表示されます。「Global」、「Radio」、「SSID」、「QoS」のタブをクリックし、プロファイルに機能の設定します。

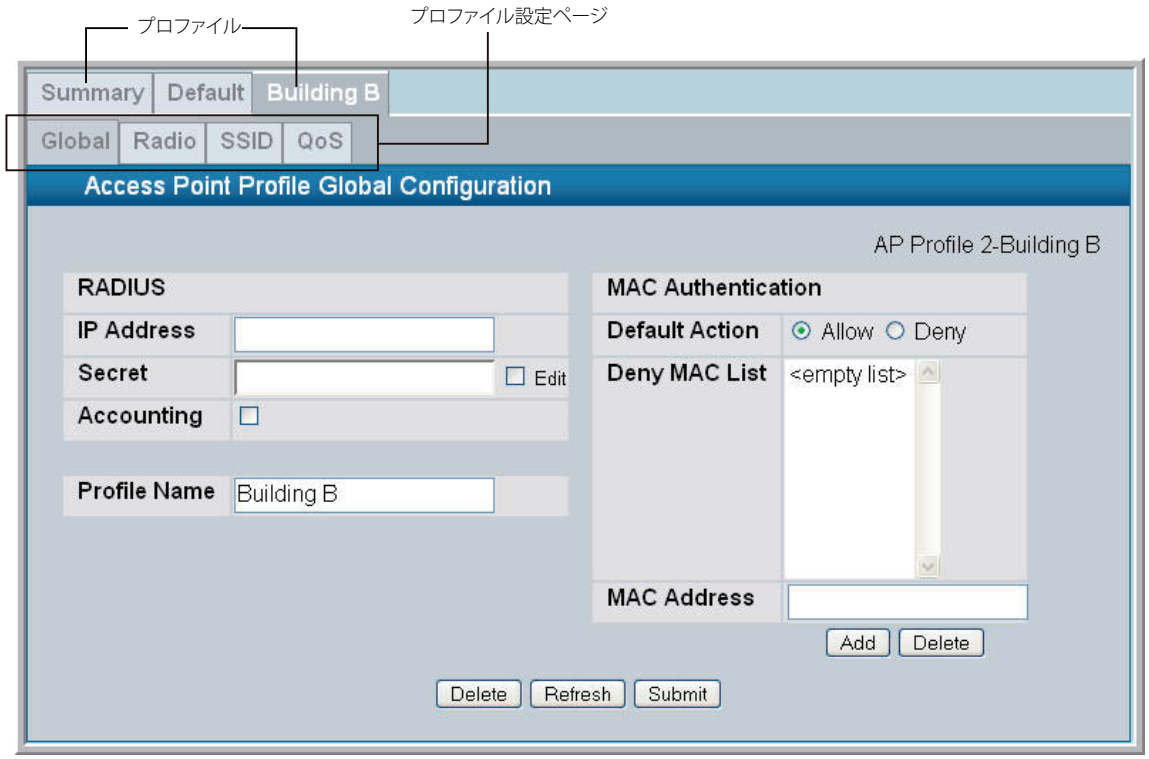


図 8-3　アクセスポイントプロファイルの設定

作成済みのプロファイルとその設定内容をコピーするためには、コピー元のプロファイルを選択し、新しいプロファイル名を入力後「Copy」ボタンをクリックします。

プロファイルを削除するためには、プロファイルを選択して「Delete」ボタンをクリックします。

作成済みのプロファイルにアクセスするためには、目的のプロファイル名のタブをクリックします。新しいプロファイルを追加すると、138 ページの「付録 A」で示す内容のデフォルト AP 設定が割り当てられています。プロファイルのコピーをすると、コピー元のプロファイルの内容が設定されます。

注意 本スイッチにより管理されているアクセスポイントが現在使用しているプロファイルは削除できません。

プロファイルの設定内容を変更するためには、「Global」、「Radio」、「SSID」、「QoS」の各タブをクリックして、各ページを表示して変更します。

「Global」ページの各項目についての詳細情報は 55 ページの「5.2 AAA と RADIUS の設定」を参照します。

「Radio」ページの各項目についての詳細情報は 57 ページの「5.3 無線電波の設定」を参照します。

「SSID」ページの各項目についての詳細情報は 61 ページの「5.4 SSID の設定」を参照します。

「QoS」ページの各項目についての詳細情報は 113 ページの「8.4 QoS の設定」を参照します。

アクセスポイントプロファイルの適用

統合スイッチ上で AP プロファイルを更新した場合、その変更内容は、そのプロファイルを使用しているアクセスポイントに自動的には適用されません。プロファイルの変更内容の適用は「Access Point Profile Summary」ページにて明示的に行うか、またはそのプロファイルを使用するアクセスポイントを再起動する必要があります。

注意 無線ネットワークの VLAN ID を変更する場合、AP は、更新したプロファイルを適用する際に一時的に DHCP に割り当てられた IP アドレスを喪失します。これが発生すると、AP は Standalone モードになります。AP がご使用のネットワークの DHCP サーバから IP アドレスを再取得すると直ちに通常操作を管理 AP として再開します。また、VAP（SSID）を有効または無効にする場合、および AP プロファイルを最適用する場合の動作を参照します。

プロファイルの変更を、そのプロファイルを使用するすべてのアクセスポイントに適用するためには、図 8-4 に示すように、プロファイルを選択して「Apply」ボタンをクリックします。

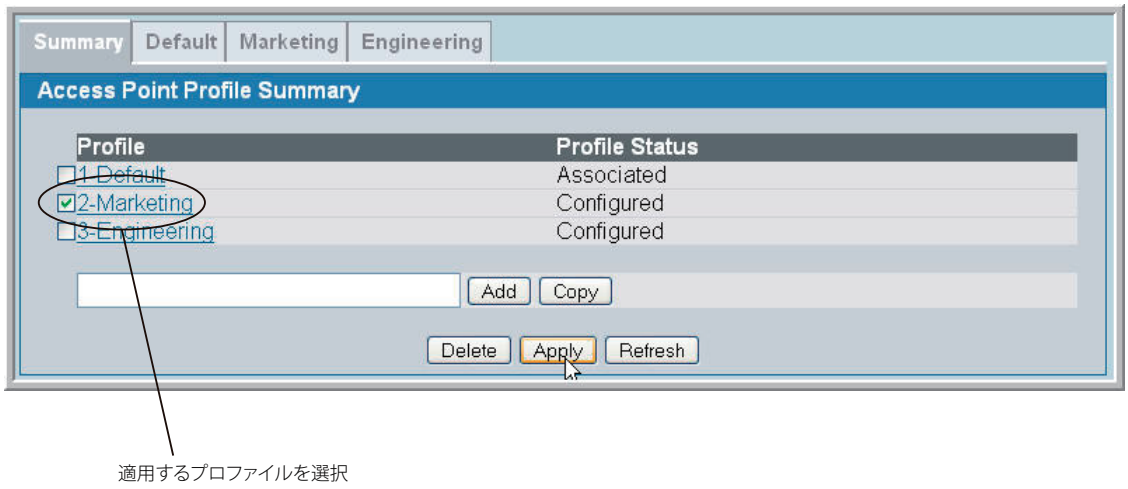


図 8-4　AP プロファイルの適用

注意 新しい AP プロファイルをアクセスポイントに適用する際、アクセスポイントは一旦停止し、システムプロセスを再開します。この時、無線クライアントは一時的に接続を失います。アクセスポイントの設定変更は、WLAN トラフィックが低い時にすることをお勧めします。

「Profile Status」欄には以下のいずれかの状態が表示されます。

項目	説明
Associated	本プロファイルは登録されており、1 台以上のスイッチ管理下のアクセスポイントにより使用されています。
Associated-Modified	本プロファイルはアクセスポイントに適用されてから内容が変更されました。再適用して、変更内容をアクセスポイントに反映する必要があります。
Apply Requested	適用リクエスト済み。プロファイルを指定して「Apply」ボタンをクリックすると、画面が更新され、この表示に変わります。
Apply In Progress	本プロファイルを使用するすべてのアクセスポイントに対して、プロファイルを適用中です。本プロセス中にアクセスポイントが再起動され、クライアントとの接続が切断されます。
Configured	本プロファイルは登録済みですが、どのアクセスポイントも本プロファイルを使用していません。

注意 プロファイルは Valid AP データベースに登録されているアクセスポイントに対して適用してください。

8.2 グローバル設定

WLAN タブ > Administration > Advanced Configuration > Global の「General」タブをクリックすると、D-Link 統合スイッチに関する設定をすることができます。

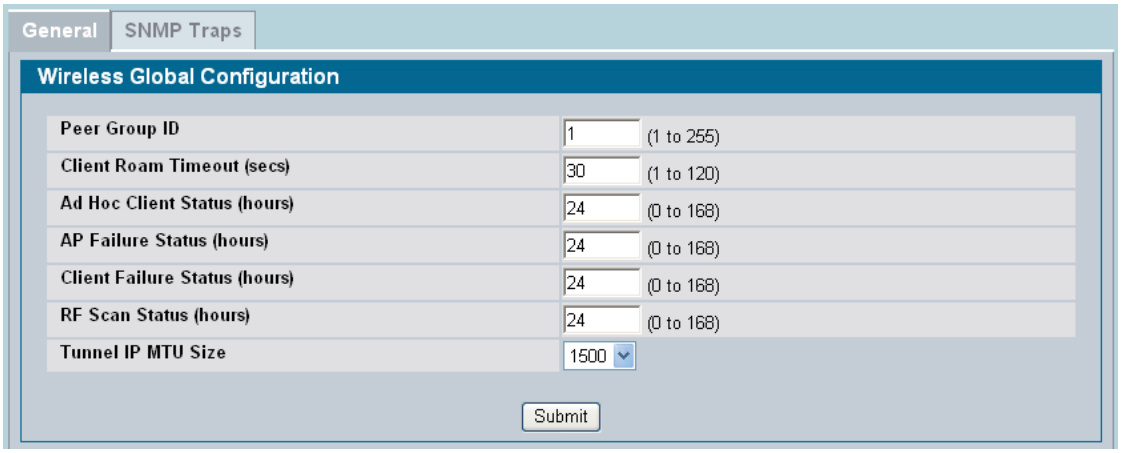


図 8-5　グローバル設定

表 8-1 に「Wireless Global Configuration」ページの各項目についての説明を示します。

表 8-1　「Wireless Global Configuration」ページ

項目	説明
Peer Group ID	大規模なネットワークを運用するために、4 台までの統合スイッチを構成したピアグループを登録することができます。ピアスイッチ同士はアクセスポイントに関する情報の一部を共有することにより L3 ローミングを実現します。 ピアはグループ ID によりグループ分けされます。
Client Roam Timeout (secs)	クライアントとアクセスポイント間の接続が切れてから、エントリが「Associated Client Status」リストから削除されるまでの時間を指定します。リストには、切断してからの経過時間（Age）が表示され、この値がここで指定した値に到達した時にそのエントリがリストから削除されます。
Ad Hoc Client Status (hours)	「Ad Hoc Client Status」リストにエントリを表示しておく時間を指定します。リストにはアドホッククライアントが検出されてからの経過時間（Age）が表示され、この値がここで指定した値に到達した時にそのエントリはリストから削除されます。
AP Failure Status (hours)	「AP Authentication Failure Status」リストにエントリを表示しておく時間を指定します。リストには認証に失敗してからの経過時間（Age）が表示され、この値がここで指定した値に到達した時にそのエントリはリストから削除されます。
Client Failure Status (hours)	「Client Authentication Failure Status」リスト内エントリを表示しておく時間を指定します。リストには認証に失敗してからの経過時間（Age）が表示され、この値がここで指定した値に到達した時にそのエントリはリストから削除されます。
RF Scan Status (hours)	「RF Scan Status」リストにエントリを表示しておく時間を指定します。リストには RF スキャンによる検出からの経過時間（Age）が表示され、この値がここで指定した値に到達した時にそのエントリはリストから削除されます。
Tunnel IP MTU Size	ネットワークに処理される IP パケットの最大サイズを設定します。MTU はトンネル VAP 上だけで実施されます。以下の 1 つを選択します。 • 1500 - トンネル IP フレームサイズ 1518 バイト（タグなし）と 1522 バイト（タグ付き）に設定します。ご使用のネットワークがジャンボフレームをサポートしない場合に本設定を使用します。トンネル IP の MTU サイズとして 1500 を使用すると D-Link 統合アクセスシステムは最大メッセージサイズを 1518/1522 バイトに制限します。本設定は、MTU 検出プロトコルを有効にし、TCP 接続設定メッセージの最大のセグメントサイズを制限することによって、フレームがオーバする問題を緩和するよう無線システムに指示します。 • 1520 - トンネル IP フレームサイズ 1538 バイト（タグなし）と 1542 バイト（タグ付き）に設定します。1538/1542 バイトのパケットをサポートするためには、ご使用のネットワークがジャンボフレームをサポートし、スイッチと AP 間の物理ポートが設定済みである場合に本設定を使用します。 L3 トンネルを使用する IP パケットには、カプセル化のためにヘッダには特別な 20 バイトがあります。これは、1500 バイトの IP MTU サイズに設定されている無線クライアントが、スイッチに 1518（1522 のタグ付き）バイトのフレームを設定し、切り換える場合に既存のネットワークインフラの最大 MTU サイズを超える可能性があることを意味します。 Network MTU Size を 1500 または 1520 を設定すると物理ポートの MTU サイズに影響しません。 スイッチと他のネットワーク装置の物理ポートは適切な MTU サイズで設定される必要があります。 **注意** AP が直接無線スイッチに接続されずに、Tunnel IP MTU Size が 1520 に設定された場合、AP と無線スイッチ間の経路にあるすべてのイーサネットセグメントがジャンボフレームをサポートし、ジャンボフレーム設定を行っている必要があります。

8.3 SNMP トラップの有効化

D-Link 統合スイッチの管理に SNMP（Simple Network Management Protocol）を使用する場合、スイッチに SNMP エージェントを設定して、ネットワーク内の SNMP マネージャにトラップ送信をする必要があります。この設定をするためには **WLAN タブ** > **Administration** > **Advanced Configuration** > **Global** とクリックし、「SNMP Traps」タブを表示します。

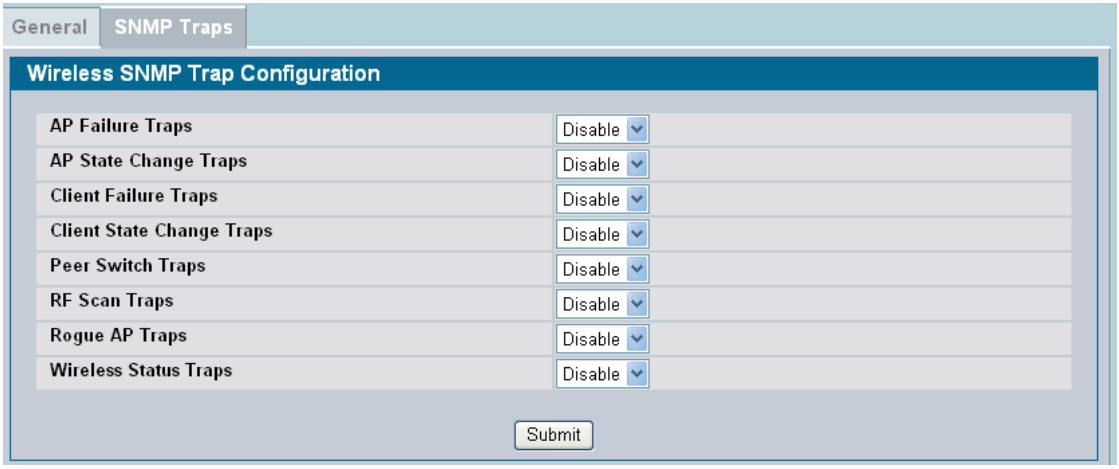


図 8-6　SNMP トラップの設定

アクセスポイントからはトラップ送信はされません。スイッチは自身のイベントと、配下のアクセスポイントからの情報更新により知ったイベントを元にトラップを生成します。

表 8-2 では SNMP トラップ送信の元となるイベントを示します。すべてのトラップは初期設定では無効に設定されています。

表 8-2　SNMP トラップ

項目	説明
AP Failure Traps	有効にすると、アクセスポイントがスイッチとの接続または認証に失敗した時に SNMP エージェントがトラップを送信します。
AP State Change	有効にすると、以下のいずれか原因により SNMP エージェントがトラップを送信します。 • 管理対象のアクセスポイントの検出。 • 管理対象のアクセスポイント異常。 • 管理対象のアクセスポイントから不明なプロトコルの検出。 • 管理対象のアクセスポイントのロードバランス使用率超過。
Client Failure Traps	有効にすると、クライアントがアクセスポイントとの接続または認証に失敗した時に SNMP エージェントがトラップを送信します。
Client State Change Traps	有効にすると、クライアントに関連する以下のいずれかの原因により、SNMP エージェントがトラップを送信します。 • クライアントの接続検出。 • クライアントの切断検出。 • クライアントのローミング検出。
Peer Switch Traps	有効にすると、ピアスイッチに関連する以下のいずれかの原因により、SNMP エージェントがトラップを送信します。 • ピアスイッチの検出。 • ピアスイッチの異常。 • ピアスイッチから不明なプロトコルの検出。
RF Scan Traps	有効にすると、RF スキャンによって新しいアクセスポイント、クライアント、またはアドホッククライアントが検出された時 SNMP エージェントがトラップを送信します。
Rogue AP Traps	有効にすると、スイッチがローグ（不正）アクセスポイントを検出した場合、SNMP エージェントがトラップを送信します。
Wireless Status Traps	有効にすると、D-Link 統合スイッチの動作状態が変化した時、または以下のデータベース中のリストのエントリ数が最大値を超えた時に SNMP エージェントがトラップを送信します。 • Managed AP データベース • AP Neighbor リスト • Client Neighbor リスト • AP Authentication Failure リスト • RF Scan AP リスト • Client Association データベース • Client Authentication Failure リスト
Client Authentication Trap	有効にすると、無線クライアントがキャプティブポータル経由のネットワーク接続のための認証に成功する場合、SNMP エージェントがトラップを送信します。

8.4 QoS の設定

D-Link 統合アクセスシステムで使用する QoS（Quality of Service）技術は、複数のキューにパラメータを指定することにより、一般的な IP データトラフィックをはじめ、VoIP（Voice-over-IP）、音声、映像、ストリーミングメディア等、さまざまな無線トラフィックのスループットとパフォーマンスの向上に効果があります。

QoS についての詳細な情報および D-Link 統合アクセスシステムにおいての QoS 活用方法については、157 ページの「付録 D QoS 制御について」を参照してください。

WLAN タブ > Administration > Advanced Configuration > AP Profiles ページでプロファイル名のタブを選択し、さらに「QoS」タブをクリックします。

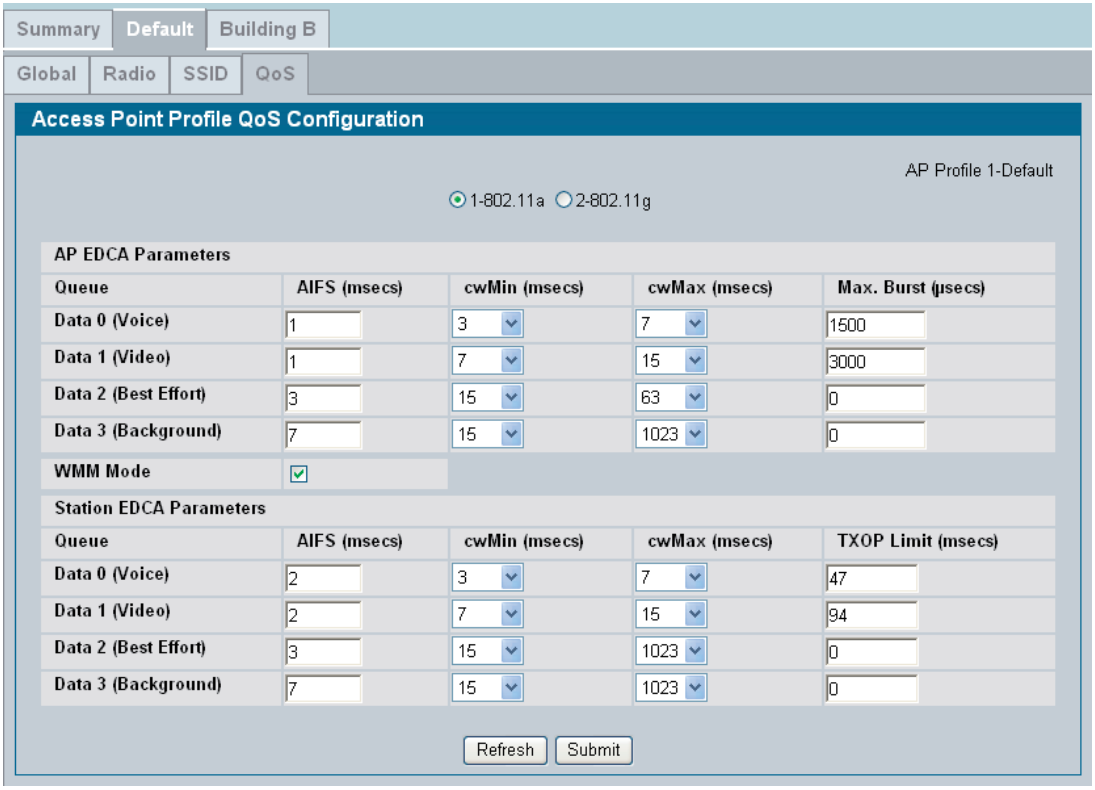


図 8-7　QoS の設定

D-Link 統合アクセスシステムで使用する QoS は、主にさまざまな種類の無線トラフィック用のキューにパラメータを設定すること、そして、伝送時の最大 / 最小待ち時間を（コンテンション画面により）効果的に指定することができます。

「AP EDCA（Enhanced Distributed Channel Access）Parameters」はアクセスポイントからクライアント向きのトラフィックフローに影響し、逆に「Station EDCA Parameters」は、クライアントからアクセスポイント向きのトラフィックフローに影響します。

注意　QoS の設定は無線インタフェースごとに行います。

表 8-3 では、QoS の設定項目について説明します。多くのパラメータは「AP EDCA」、「Station EDCA」で共通です。

表 8-3　QoS 設定項目

項目	説明
Queue Data 0 (Voice) Data 1 (Video) Data 2 (Best Effort) Data 3 (Background)	アクセスポイントからクライアントに送信するデータのタイプごとにキューを定義します。 • Data 0（音声）- 最高優先度キュー、最小遅延。遅延に敏感な VoIP やストリーミングメディアなどのデータは自動的に本キューに送られます。 • Data 1（ビデオ）- 高優先度キュー、最小遅延。遅延に敏感なビデオデータは自動的に本キューに送られます。 • Data 2（ベストエフォート）- 中優先度キュー、中スループット。一般的な IP データは本キューに送られます。 • Data 3（バックグラウンド）- 低優先度キュー、高スループット。高いスループットを要する大容量データや、遅延に敏感ではないデータは本キューに送られます（例 : FTP データなど）。
AIFS （Inter-Frame Space）	AIFS（Arbitration Inter-Frame Spacing）では、データフレーム間の待ち時間を指定します。1 から 255 の間の値を指定します。単位はミリ秒です。

項目	説明
cwMin（Minimum Contention Windows）	本パラメータは、伝送リトライの「初回ランダムバックオフ待ち時間」（画面）を定義するアルゴリズムに使用します。本値は、「初回ランダムバックオフ待ち時間」の範囲の上限として指定します。単位はミリ秒です。1 番目のランダム（任意）番号は、0 からここで指定する値の中から生成されます。 データフレームが送信される前に、1 番目のランダムバックオフ待ち時間が失効すると、リトライカウンタは 1 増加し、ランダムバックオフ値（画面）は 2 倍の値になります。このランダムバックオフ値が、次の項目の cwMax で定義する値に到達するまで、失効に伴って値を倍にしていきます。 cwMin には 1、3、7、15、31、63、127、255、511、1023 のいずれかの値を指定してください。 本欄には cwMax で定義する値と同じか小さい値を指定してください。
cwMax（Maximum Contention Windows）	本パラメータは、ランダムバックオフ値の上限です。ランダムバックオフ値は、データフレームが送信されるか、ここで指定した値に到達するまで、倍掛けされていきます。単位はミリ秒です。 ランダムバックオフ値が、ここで指定した値に到達すると、リトライは「リトライ許可最大回数」に到達するまで継続されます。 1、3、7、15、31、63、127、255、511、1024 のいずれかの値を指定してください。 cwMin で定義する値より大きい値を指定してください。
Max.Burst Length	最大バースト長。AP EDCA パラメータ用のみ（ここで指定する値はアクセスポイントからクライアントへのトラフィックに対してのみ適用されます）。 本値は無線ネットワークでのパケットバーストに認められる最大バースト長です。パケットバーストとはヘッダ情報なしで送信できる複数のフレームの集まりです。 オーバヘッドを少なくすることにより、高スループットと高パフォーマンスを実現できます。 本値の入力範囲は、0.0 から 999.9 です。
WMM Mode	WMM（Wi-Fi Multimedia）機能は、初期値では有効になっています。WMM が有効であると、QoS 優先制御や無線メディアアクセスの調整も有効になります。また D-Link 統合アクセスシステムの QoS 設定は上りと下り両方のトラフィック（クライアントからアクセスポイント [Station EDCA パラメータ]、およびアクセスポイントからクライアント [AP EDCA パラメータ]）に対して有効になります。 WMM を無効に設定すると、QoS 制御は上りのトラフィック（クライアントからアクセスポイント [Station EDCA パラメータ]）に対して無効になります。下りについては、いくつかのパラメータ [AP EDCA パラメータ] の設定は有効です。 WMM 機能を無効にするためには「Disabled」を、有効にするためには「Enabled」を選択してください。
TXOP Limit	Station EDCA パラメータ（クライアントからアクセスポイントへの上りトラフィック）のみの設定です。TXOP（Transmission Opportunity: 送信権）は、WME クライアントが無線メディア上で送信を始める権利が発生する間隔です。ここで設定した間隔（ミリ秒）で、WMM クライアントは無線ネットワーク上に送信する権利を与えられます。TXOP Limit 範囲は 0-65465 です。値は 32μ 秒単位です。

第 9 章　キャプティブポータル設定

キャプティブポータル（CP : Captive Portal）機能により、ユーザ検証が確立されるまで無線クライアントのネットワークへのアクセスを防御します。

本章は以下の項により構成し、D-Link 統合アクセスシステムネットワークの CP 機能の設定およびモニタを行います。

項目	説明	参照ページ
グローバルキャプティブポータル設定	スイッチに設定済みの全キャプティブポータルに影響するグローバル設定を行います。	115 ページ
キャプティブポータル設定	キャプティブポータルに関するサマリ情報の参照、キャプティブポータルの追加または削除をします。	116 ページ
キャプティブポータルユーザのモニタと設定	ローカルデータベース内のキャプティブポータルユーザの参照または設定を行います。	120 ページ
インタフェースへのキャプティブポータルの割り当て	特定の無線ネットワーク（SSID）に設定したキャプティブポータルを関連付けます。	122 ページ
キャプティブポータルステータスの参照	キャプティブポータルステータス情報を参照します。	123 ページ
クライアントサマリの参照	キャプティブポータルを経由して D-Link 統合アクセスシステムに接続する無線クライアントに関する情報を参照します。	126 ページ
SNMP トラップの設定	各種のキャプティブポータル機能に SNMP トラップ設定を行います。	129 ページ

CLI を使用してアクセスポイントの保守管理をするためのコマンドの詳細については、「D-Link CLI MANUAL」を参照してください。

注意　キャプティブポータル設定画面は、LAN および WLAN タブ両方のセキュリティフォルダから表示することができます。

9.1 グローバルキャプティブポータル設定

「CP Global Configuration」ページで、CP 機能の管理用ステータスを制御し、スイッチに設定されたすべてのキャプティブポータルに影響するグローバル設定を行います。

グローバル CP 設定を行うためには、**WLAN タブ > Security > Captive Portal > Global Configuration** の順にメニューをクリックします。

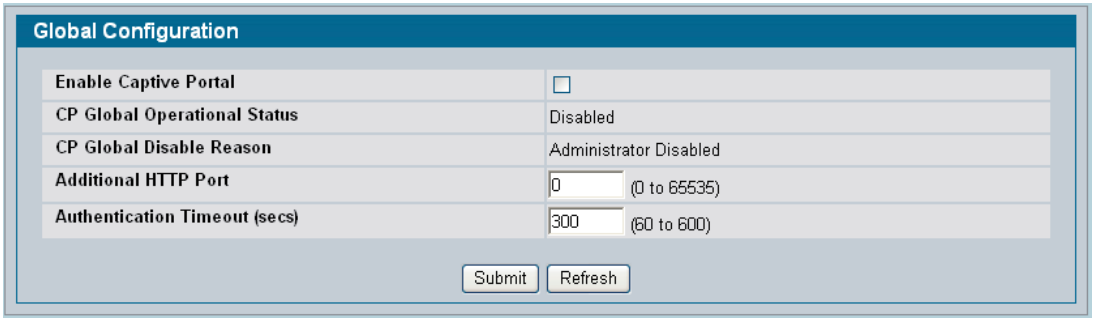


図 9-1　Global Configuration 画面

表 9-1 では参照、または設定可能なグローバル CP の項目について説明しています。

表 9-1　　グローバルキャプティブポータル設定

項目	説明
Enable Captive Portal	チェックボックスを選択して、スイッチの CP 機能を有効にします。キャプティブポータル機能を無効にするためには、チェックを外してください。
CP Global Operational Status	CP 機能が有効かどうかを表示します。
CP Global Disable Reason	CP が無効の場合、以下の原因から一つが表示されます。 • None - 以下のいずれでもない状態です。 • Administratively Disabled - 管理上無効です。 • No IPv4 Address - IPv4 アドレスではありません。 • Routing Enabled, But no IPv4routing interface - ルーティングが有効ですが、IPv4 ルーティングインタフェースではありません。
Additional HTTP Port	HTTP トラフィックはポート 80 を使用しますが、HTTP トラフィックに追加ポートを設定することができます。0-65535（ポート 80 は除く）のポート番号を入力します。
Authentication Timeout (secs)	ポータル経由でネットワークにアクセスするために、無線クライアントははじめに認証 Web ページに認証情報を入力する必要があります。認証セッションをクライアントと共にオープンしておく時間（秒）。タイムアウト時間になると、スイッチは、クライアントと接続するどんなアクティブな TCP や SSL も切断します。

9.2 キャプティブポータルの設定

キャプティブポータル設定の作成、削除

「CP Summary」ページを使用してキャプティブポータル設定の作成、または削除をします。スイッチは、10 個の CP 設定をサポートしています。CP 設定の 1 はデフォルトで作成されて、削除することはできません。各キャプティブポータル設定には、固有のゲストまたはグループのアクセスモードとカスタマイズされた承認があり、クライアントが接続する場合に表示するポリシーを使用できます。

キャプティブポータルに関するサマリ情報の参照、キャプティブポータルの追加または削除のためには、**WLAN タブ > Security > Captive Portal > CP Configuration** の順にメニューをクリックします。

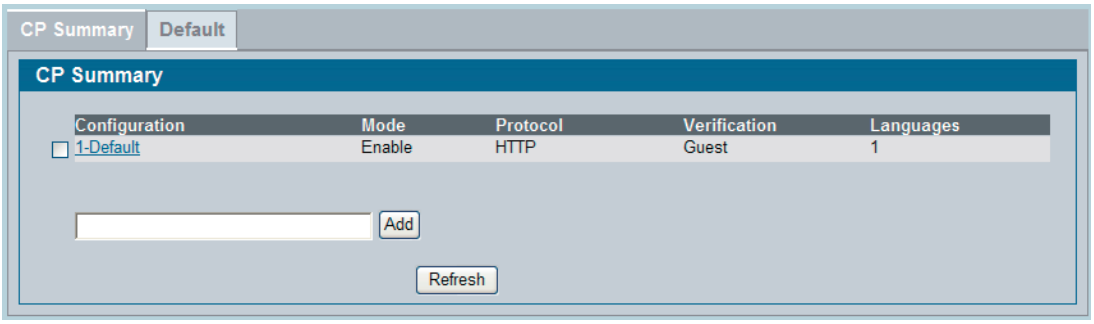


図 9-2　CP Summary 画面

既存の CP を削除するためには、削除する CP にチェックを入れ、「Delete」ボタンをクリックします。
既存の CP 設定を変更するためには、「Configuration」欄の名前をクリックし、対応するタブをクリックします。

表 9-2 は「CP Summary」ページの各項目を説明します。

表 9-2　Captive Portal Summary

項目	説明
Configuration	キャプティブポータル ID と名前を表示します。定義済み CP の設定ページにアクセスするためには、設定名をクリックします。
Mode	CP が有効か否かを表示します。
Protocol	ポータルが HTTP か HTTPS を使用するか否かを表示します。
Verification	実行するユーザ検証のタイプを指定します。 • Guest - ユーザは、データベースによって認証される必要はありません。 • Local - スイッチは、認証ユーザに対してローカルデータベースを使用します。 • RADIUS - スイッチは、ユーザを認証するためにリモート RADIUS サーバのデータベースを使用します。 ローカルまたはリモートな RADIUS データベースで認証ユーザを設定するためには、120 ページの「9.3 キャプティブポータルユーザのモニタと設定」を参照してください。
Languages	設定している言語数を表示します。

キャプティブポータル設定の変更

初期値では、D-Link 統合スイッチには、1 つのキャプティブポータルがあります。キャプティブポータルの設定変更、または 9 個までの追加ポータルを設定すること尾ができます。「CP Summary」ページでキャプティブポータルを作成後に設定を変更することができます。

WLAN タブ > Security > Captive Portal > CP Configuration の順にメニューをクリックし、「CP Summary」画面で編集する「Configuration」のリンクをクリックします。

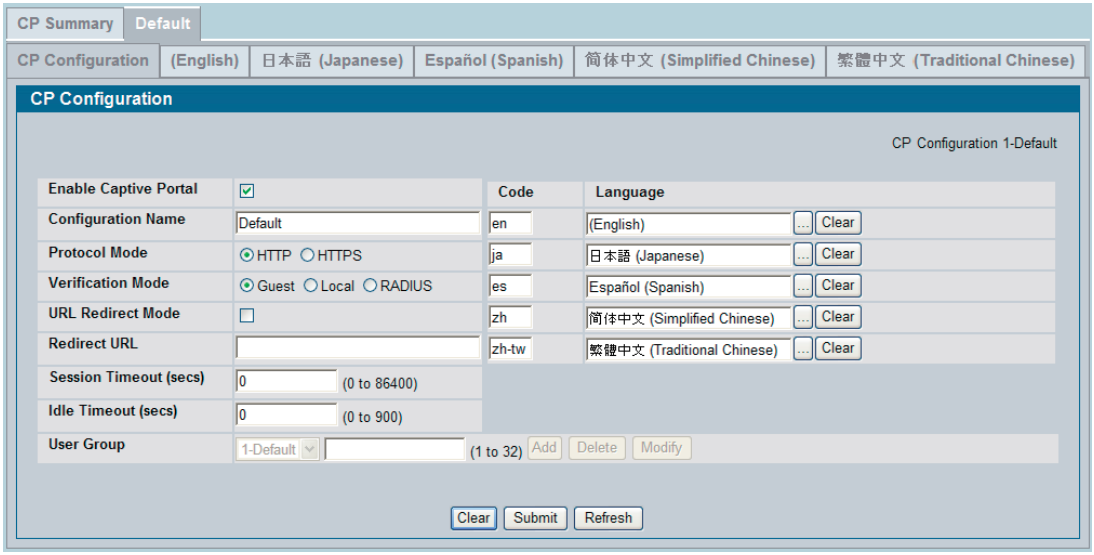


図 9-3　CP Configuration 画面

表 9-3 では「CP Configuration」ページの各項目の詳細を説明します。

表 9-3　CP 設定

項目	説明
Enable Captive Portal	チェックボックスを選択して、CP を有効にします。チェックを外して、機能を無効にします。
Portal Configuration Name	CP Summary ページで追加されたポータル名を変更することができます。
Protocol Mode	検証プロセスの間に使用するポータルために使用するプロトコル（HTTP または HTTPs）を選択します。 • HTTP - 検証の間、暗号を使用しません。 • HTTPS - Secure Sockets Layer（SSL）を使用し、これは証明書が暗号化を提供することを必要とします。証明書は接続時にユーザに提示されます。
Verification Mode	クライアントを認証するために、CP のモードを選択します。 • Guest - ユーザは、データベースに認証される必要がありません。 • Local - スイッチは認証ユーザに対してローカルデータベースを使用します。 • RADIUS - スイッチは、ユーザを認証するためにリモート RADIUS サーバのデータベースを使用します。
URL Redirect	チェックボックスを選択して、CP が新たに認証されたクライアントを設定した URL にリダイレクトするように指定します。チェックボックスがクリアされると、検証の成功後に指定したウェルカムページが表示されます。
Redirect URL	URL Redirect Mode が有効にされると、新たに認証されたクライアントがリダイレクトされる URL を指定します。
Session Timeout	セッション終了前の待機時間（秒）。セッションタイムアウトになると、ユーザはログアウトされます。値が 0 に設定されると、タイムアウトにはなりません。初期値は 0 です。
Idle Timeout	自動的にログアウトされるまでユーザが待機できる時間（秒）を入力します。値が 0 に設定されると、タイムアウトにはなりません。初期値は 0 です。 **注意** アイドルタイムアウトは、有線クライアントには使用できません。
User Group	Verification Mode が Local または「RADIUS」の場合、既存のユーザグループをキャプティブポータルに割り当てるか、または新しいグループを作成します。グループに所属するすべてのユーザが、このポータル経由でネットワークにアクセスすることが許可されます。User Group リストは、スイッチのすべての CP 設定で同じです。 「User Group」欄では、すべてのキャプティブポータルに対するユーザグループの追加、削除または名前の変更ができます。プルダウンメニューから CP に割り当てる定義済みユーザグループを選択します。 • 新しいユーザグループを作成するためには、「User Group」欄にグループ名を入力し、「Add」ボタンをクリックします。 • 既存のユーザグループ名を変更するためには、プルダウンメニューから変更する名前を選択し、新しい名前を空白の欄に入力して、「Modify」ボタンをクリックします。 • ユーザグループを削除するためには、プルダウンメニューから削除する名前を選択し、「Delete」ボタンをクリックします。 **注意** 「Verification Mode」が「Guest」の場合、「User Group」欄は使用できません。
Code	言語に対して IANA 言語サブタグコードを入力します。すべてのコードが IANA 言語サブタグレジストリに表示されます。スイッチに言語がサポートされている場合、言語を選択するとコードが自動的に入力されます。

項目	説明
Language	スイッチがサポートする言語にキャプティブポータル設定を追加するためには、「...」ボタンをクリックしてキャプティブポータルに使用する言語を表示、選択します。キャプティブポータル設定の言語を削除するためには、「Clear」ボタンをクリックします。
Acceptance Use Policy	ユーザが CP にアクセスする場合、表示する「Acceptance Use Policy」を入力します。ポリシーは 8192 文字のテキストを含むことができます。

キャプティブポータル Web ページのカスタマイズ

クライアントが有線またはアクセスポイントを経由してスイッチに接続すると、キャプティブポータル Web ページが表示されます。「CP Web Page Customization」画面では、特定の文字や画像で画面のカスタマイズをすることができます。

すべてのページが同じ認証タイプを使用していれば、それぞれのキャプティブポータルに対し最大 5 つのローカル Web 画面（ゲストまたは認定ユーザ用 Web 画面）を作成することができます。これによってさまざまな言語で画面を作成することが可能となり、異なるグループやユーザに適応することができます。

有線および無線クライアントがキャプティブポータルに接続した時に参照する画面をカスタマイズするためには、対応する画面の言語タブをクリックして設定します。

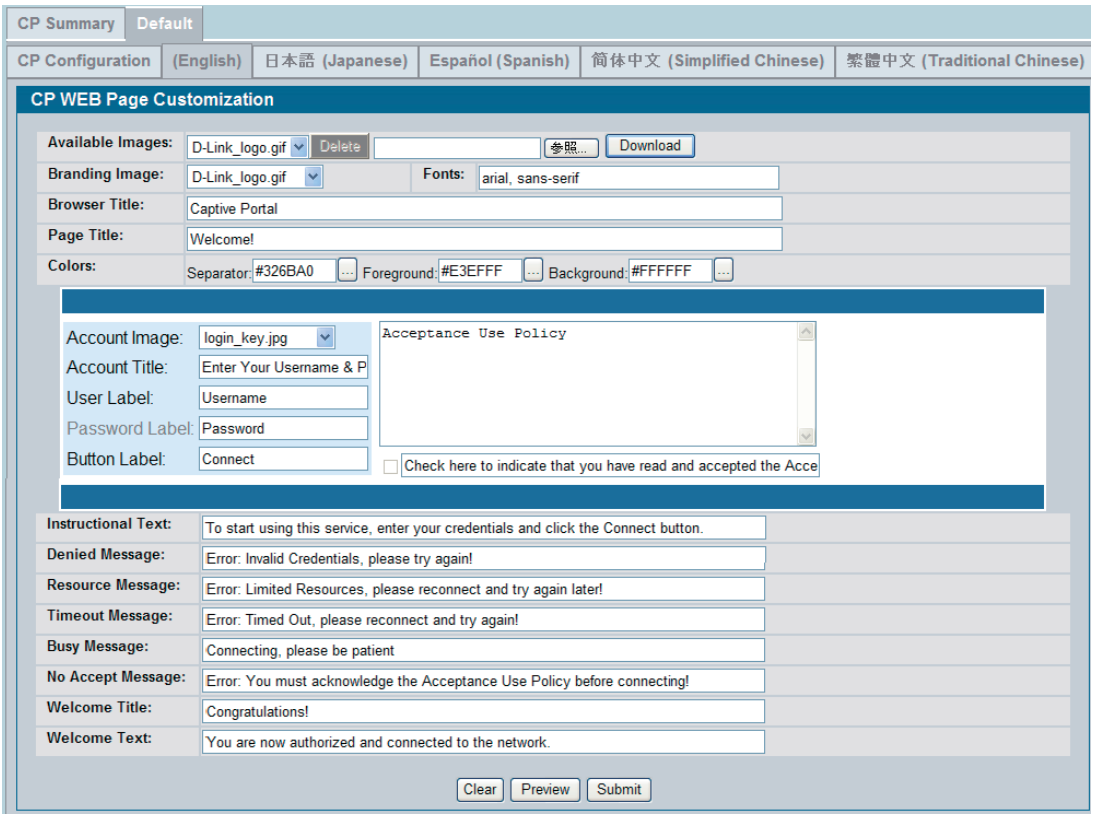


図 9-4　CP Web Page Customization 画面

以下の表に「CP Web Page Customization」画面の各項目について示します。

項目	説明
Available Images	メニューには画面タイトルおよびアカウント画像に使用できる画像が表示されます。画像を追加する場合は、「Browse」ボタンをクリックし、ご使用のローカルシステムの画像、またはローカルシステムからアクセスできる画像を選択します。「Download」ボタンをクリックすると、画像のダウンロードを開始します。 画像は最大 5KB、200x200 画素、GIF または JPG 形式とします。 リストから画像を削除する場合は、プルダウンメニューからそのファイル名を選択して「Delete」ボタンをクリックします。削除できるのはダウンロードした画像のみです。
Branding Image	画像ファイル名を選択すると、画面左上に表示されます。この画像は会社のロゴなどのようなブランド表示の目的に使用します。
Fonts	CP 画面の全テキストに使用するフォント名を入力します。
Browser Title	クライアントの Web ブラウザのタイトルバーやタブに表示するテキストを入力します。
Page Title	画面タイトルとして使用するテキストを入力します。これは、画面を識別するテキストです。
Colors	CP 画面に使用する色を選択します。「...」ボタンをクリックして、使用する色を選択します。選択した色でサンプルアカウント情報が更新されます。
Account Image	キャプティブポータル画面でログイン欄の上部に表示する画像を選択します。スイッチに新しい画像をダウンロードするためには、「Available Image」欄を使用します。
Account Title	ユーザに認証を指示するサマリテキストを入力します。
User Label	ユーザ名入力欄の横に表示するテキストを入力します。
Password Label	パスワード入力欄の横に表示するテキストを入力します。
Button Label	ネットワークに接続する時にクリックするボタンに表示するテキストを入力します。
Acceptance Use Policy Text Box	「Acceptance Use Policy」欄に表示するテキストを入力します。「Acceptance Use Policy」は、ユーザがネットワークへの接続を許可されている時にその状況を示します。ポリシーは 8192 文字のテキストを含むことができます。
Acceptance Check Box Prompt	ユーザが使用条件を承諾したことを示すために選択する必要があるボタンの横に表示するテキストを入力します。
Instructional Text	ユーザに認証を行うよう指示する詳細なテキストを入力します。このテキストはボタンの下に表示されます。
Denied Message	ユーザが有効な認証情報を提供しない場合に表示するテキストを入力します。 このメッセージは、ユーザが CP 設定画面経由で割り当てられるユーザグループのメンバでない場合にも表示されます。 このメッセージは、ネットワークに接続するためにユーザがボタンをクリックした後に表示されます。
Resource Message	システムリソースの制限のために、システムが認証を拒否した場合に表示するテキストを入力します。このメッセージは、ネットワークに接続するためにユーザがボタンをクリックした後に表示されます。
Timeout Message	認証トランザクションに時間がかかりすぎたことによりシステムが認証を拒否した場合に表示されるテキストを入力します。これはユーザの入力時間、または全体のトランザクションのタイムアウト時に表示されます。
Busy Message	キャプティブポータル機能が認証リクエストを処理している時に表示されるテキストを入力します。このメッセージは、ネットワークに接続するためにユーザがボタンをクリックした後に表示されます。
No Accept Message	ユーザが「Acceptance Use Policy」を承諾しなかった場合に表示するテキストを入力します。このメッセージは、ネットワークに接続するためにユーザがボタンをクリックした後に表示されます。
Welcome Title	ネットワークへの接続に成功した後に表示するユーザへの挨拶テキストを入力します。
Welcome Text	CP ユーザがアクセスするネットワークの詳細を確認するためのオプションテキストを入力します。このメッセージは「Welcome Title」の下に表示されます。

画面下部のボタンを使用して次のようなタスクを行います。

- 「Clear」ボタンをクリックし、画面を初期設定にリセットします。
- 「Preview」ボタンをクリックし、カスタマイズした画面をプレビューします。
- 「Submit」ボタンをクリックし、変更をスイッチに適用します。

9.3 キャプティブポータルユーザのモニタと設定

ローカルデータベースの CP ユーザの参照または設定

ゲストユーザと認証ユーザに対応するポータルを設定します。ゲストユーザにはユーザ名およびパスワードの割り当てはありません。認証ユーザには、はじめにローカルデータベースまたは RADIUS サーバに認証されるべき有効なユーザ名とパスワードがあります。D-Link 統合スイッチが一度ユーザの証明書を確認すると、認証されたユーザはネットワークへのアクセス権を取得します。

「Local User Summary」ページでは、ローカルデータベースに認証ユーザを追加します。1024 までのユーザエントリを追加できます。また、「Local User Summary」でローカルデータベースからユーザを削除することもできます。

ローカルデータベース内の CP ユーザの参照または設定を行うためには、**WLAN タブ > Security > Captive Portal > Local User** の順にメニューをクリックします。

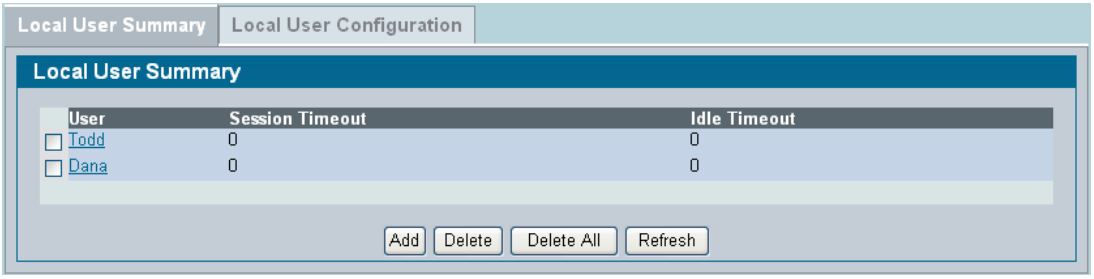


図 9-5　Local User Summary 画面

表 9-4 は「Local User Summary」ページの各項目を説明します。

表 9-4　Local User Summary

項目	説明
User	ユーザ名を指定します。
Group	ユーザが所属するグループ名を指定します。各キャプティブポータルには、ユーザグループが割り当てられます。グループ内のユーザだけがキャプティブポータルにアクセスできます。 各ユーザは 1 つ以上のグループに所属することができます。
Session Timeout	ユーザがネットワークに接続されたままで残っていることを許容される時間（秒）を表示します。「Session Timeout」値に到達すると、ユーザは自動的にログアウトされます。0 は、ユーザが「Session Timeout」制限を持たないことを意味します。
Idle Timeout	自動的にログアウトされるまでユーザが待機できる時間（秒）を示します。0 は、ユーザが自動的にログアウトされないことを意味します。 注意 アイドルタイムアウトは、有線クライアントには使用できません。

画面下部のボタンを使用して、以下のタスクを行います。

- 指定ユーザの設定ページにアクセスするためには、ユーザ名をクリックします。
- 新規ユーザを登録し、ローカルユーザ設定を行うためには、「Add」ボタンをクリックします。
- ローカルデータベースからユーザを削除するためには、削除するユーザの左側にあるチェックボックスを選択して「Delete」ボタンをクリックします。
- 複数のチェックボックスを選択し、一度に 1 人以上のユーザを削除します。「Delete All」ボタンをクリックして、ローカルデータベースからすべての設定ユーザを削除します。

ローカルデータベースへのユーザ設定

「Local User Configuration」ページでローカルデータベース内の定義済み CP ユーザに追加設定を設定できます。

WLAN タブ > Security > Captive Portal > Local User の順にメニューをクリックします。「Local User Summary」タブの「Local User Configuration」画面で「Add」ボタンをクリックし、「Local User Configuration」画面を表示します。

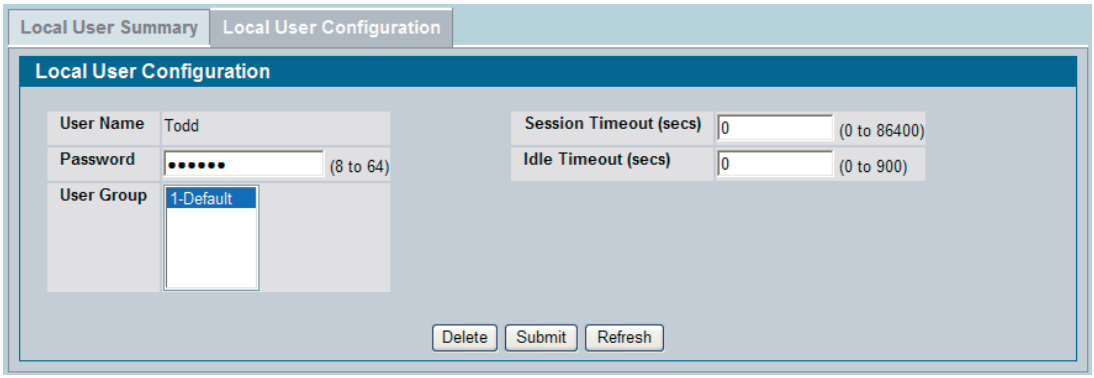


図 9-6　Local User Configuration 画面

「User Name」と「Password」を入力し、「User Group」を選択して、「Add」ボタンをクリックします。

表 9-5 ではローカルデータベースに CP ユーザを設定するために使用する項目について説明します。

表 9-5　Local User Configuration

項目	説明
User Name	ユーザ名を指定します。
Password	ユーザのパスワードを入力します。（8-64 文字。）
User Group	少なくとも 1 つのユーザグループにユーザを割り当てます。複数のグループにユーザを割り当てるためには、「Ctrl」キーを押して、各グループをクリックします。新しいユーザは、初期値では 1-Default のユーザグループに割り当てられます。
Session Timeout	ユーザがネットワークに接続されたままでいることを許容されている時間（秒）を入力します。「Session Timeout」値に到達すると、ユーザは自動的にログアウトされます。0 は、ユーザが「Session Timeout」制限を持たないことを意味します。
Idle Timeout	自動的にログアウトされるまでユーザが待機できる時間（秒）を入力します。0 は、ユーザが「Session Timeout」制限を持たないことを意味します。 注意 アイドルタイムアウトは、有線クライアントには使用できません。

リモート RADIUS サーバにユーザを設定する

リモート RADIUS サーバクライアント認証を使用することができます。すべてのユーザを RADIUS サーバに追加する必要があります。D-Link 統合スイッチにおけるローカルデータベースとは情報を共有しません。

表 9-6 は、認証済みのキャプティブポータルクライアントを設定するために使用する RADIUS 属性を示しています。本テーブルは RADIUS 属性とベンダ特有の属性（VSA）の両方を示しています。VSA は、「Attribute」欄に表示され、「,」カンマで区切られています。（例 vendor id, attribute id）

表 9-6　キャプティブポータルユーザ RADIUS 属性

属性	番号	説明	範囲	使用方法	初期値
User-Name	1	認証されるユーザ名。	1-32 文字の半角英数字。	必要な場合。	なし。
User-Password	2	ユーザパスワード。	8-64 文字。	必要な場合。	なし。
DLink-Captive-Portal-Groups	6132, 127	設定した「CP instance configuration」に対応するグループ名をコンマで区切っているリスト。	文字列。	オプション。	なし。指定しない場合は、初期設定が使用されます。
Session-Timeout	27	セッションタイムアウトに到達するとログアウトします。属性が 0 または表示されていない場合、キャプティブポータルに設定された値を使用します。	整数（秒）。	オプション。	0
Idle-Timeout	28	アイドルタイムアウトに到達するとログアウトします。属性が 0 または表示されていない場合、キャプティブポータルに設定された値を使用します。	整数（秒）。	オプション。	0

9.4 インタフェースへのキャプティブポータルの割り当て

「Interface Association」ページでは、特定の物理的インタフェースや無線ネットワーク (SSID) に設定したキャプティブポータルを関連付けることができます。CP 機能は、指定する有線または無線インタフェースで動作します。

注意 キャプティブポータル設定に物理的インタフェースを関連させる場合、以下のような制限があります。

- キャプティブポータルと STP を同じ物理的インタフェース上で有効にすることはできません。
- キャプティブポータルと 802.1X を同じ物理的インタフェース上で有効にすることはできません。
- ポートセキュリティとキャプティブポータルを同じ物理的インタフェース上で有効にすることはできません。
- 物理的インタフェースが LAG メンバである場合、キャプティブポータルはそのインタフェース上では無効になります。

インタフェースに CP を割り当てるためには、**WLAN タブ > Security > Captive Portal > Interface Association** の順にメニューをクリックします。

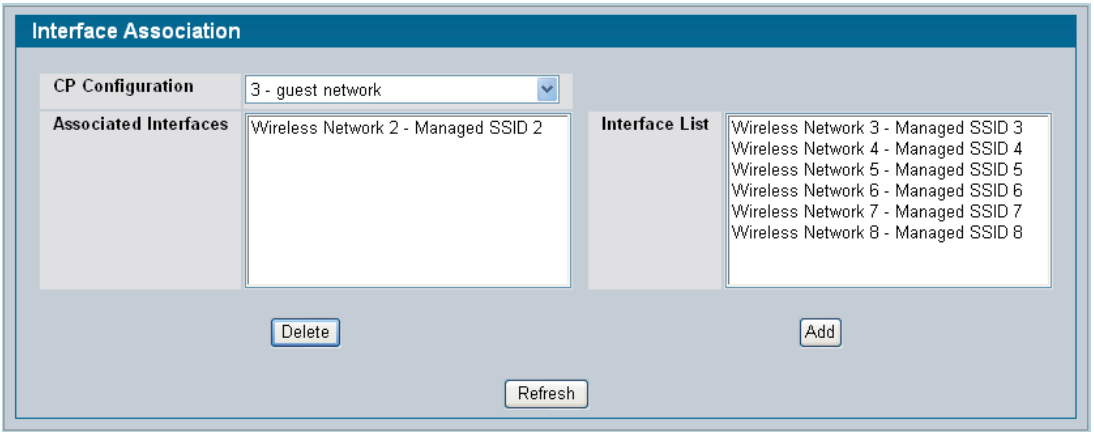


図 9-7　Interface Association 画面

表 9-7 は「Interface Association」ページの各項目の詳細を説明します。

表 9-7　グローバルキャプティブポータル設定

項目	説明
CP Configuration	スイッチに設定されたキャプティブポータルを番号と名前ごとに表示します。
Associated Interfaces	選択されたキャプティブポータルに関連する無線インタフェースを示します。無線インタフェースは、無線ネットワーク番号と SSID により識別されます。物理的（有線）インタフェースは、スロット番号、ポート番号およびインタフェースタイプを含むポート種別により識別されます。
Interface List	現在 CP に関連付けされていないスイッチで利用可能な無線インタフェースを示します。無線インタフェースは、無線ネットワーク番号と SSID により識別されます。物理的（有線）インタフェースは、スロット番号、ポート番号およびインタフェースタイプを含むポート種別により識別されます。

以下のステップを使用して、1 つ以上のインタフェースをキャプティブポータルに関連付けします。

1. 「CP Configuration」リストから希望のキャプティブポータルを選択します。
2. インタフェースリストから 1 つ以上のインタフェースを選択します。複数のインタフェースを選択するためには、「Ctrl」キーを押したまま、複数のインタフェースをクリックします。
3. 「Add」ボタンをクリックします。

注意 キャプティブポータルにインタフェースを関連させる時、そのインタフェースは「Interface List」から削除されます。各インタフェースは一度に 1 つの CP にだけ関連付けされます。

以下の手順を使用して、キャプティブポータルのために「Associated Interfaces」リストからインタフェースを削除します。

1. 「CP Configuration」リストから希望のキャプティブポータルを選択します。
2. 「Associated Interfaces」欄で削除するインタフェースを選択します。複数のインタフェースを選択するためには、「Ctrl」キーを押したまま、複数のインタフェースをクリックします。
3. 「Delete」ボタンをクリックします。

インタフェースは、「Associated Interface」リストから削除されて、インタフェースリストに表示されます。

9.5 キャプティブポータルステータスの参照

キャプティブポータルのグローバルステータスの参照

「CP Global Status」ページには CP 機能に関するさまざまな情報があります。「CP Global Status」ページから、CP の動作およびインタフェースに関する情報にアクセスできます。

キャプティブポータルステータス情報を参照するためには、**WLAN タブ > Security > Captive Portal > CP Status** の順にメニューをクリックし、「Global Status」タブを参照します。

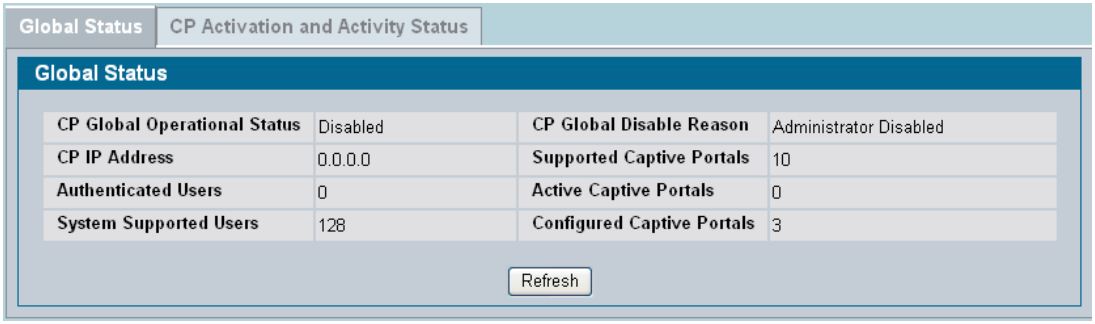


図 9-8　Global Status 画面

表 9-8 では「CP Global Status」ページ内の各項目について説明します。

表 9-8　グローバルキャプティブポータルステータス

項目	説明
CP Global Operational Status	CP 機能が有効かどうかを表示します。
CP Global Disable Reason	CP が無効の場合、無効にされた理由を表示します。以下のいずれかが表示されます。 • None - 以下のいずれでもない状態です • Administratively Disabled - 管理上無効です • No IPv4 Address - IPv4 アドレスではありません • Routing Enabled、But no IPv4routing interface - ルーティングが有効ですが、IPv4 ルーティングインタフェースではありません この項目は、CP の操作上のステータスが「Enabled」（有効）である場合にだけ表示されます。
CP IP Address	キャプティブポータルの IP アドレスを表示します。
Authenticated Users	本スイッチにおけるすべてのキャプティブポータルインスタンスに対して認証されているユーザ数を表示します。
System Supported Users	システムがサポートしている認証ユーザの数を表示します。
Configured Captive Portals	スイッチに設定されたキャプティブポータル数を表示します。
Supported Captive Portals	システムのサポートしているキャプティブポータルの数を表示します。
Active Captive Portals	操作上有効であるキャプティブポータルインスタンスの数を表示します。

CP アクティベーションと動作のステータスの参照

「CP Activation and Activity Status」ページは、スイッチに設定されている各 CP に関する情報を提供します。

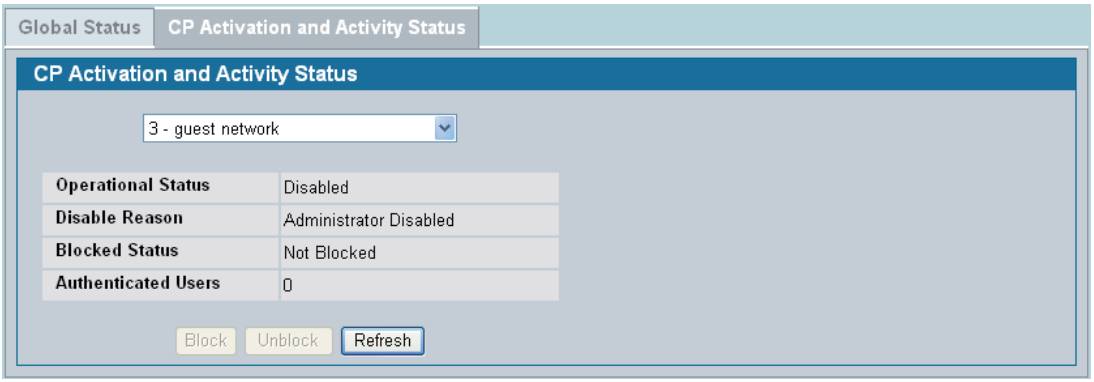


図 9-9　CP Activation and Activity Status 画面

「CP Activation and Activity Status」ページには、スイッチに設定されているすべてのキャプティブポータルを含むプルダウンメニューがあります。キャプティブポータルを選択する場合、そのポータルのためのアクティベーションと動作のステータスを表示します。

表 9-9 は各ポータルに対する情報について説明します。

表 9-9　CP Activation and Activity Status

項目	説明
Operational Status	キャプティブポータルの有効または無効を表示します。
Disable Reason	キャプティブポータルが無効の場合、この欄はその理由を表示します。ポータルインスタンスは以下の理由で無効になった可能性があります。 • None - CP が有効です。 • Administratively Disabled - 管理上無効です。 • RADIUS Authentication mode enabled, but RADIUS server is not defined. - RADIUS 認証モードが有効にされましたが、RADIUS サーバは定義されていません。 • Not associated with any interfaces. - どのインタフェースにもワークに関連付けされていません。 • The associated interfaces do not exist or do not support the CP capability. - 割り当てられたインタフェースが存在しないか、または CP 機能をサポートしていません。
Blocked Status	キャプティブポータルへの認証の試みが現在防御されているか否かを表示します。 「Block」と「Unblock」ボタンを使用して、防御ステータスを制御します。CP が防御されると、ユーザは CP を経由したネットワークへのアクセスを行うことができません。本機能を使用して、DoS 攻撃などの予期しないイベントの間、一時的にネットワークを保護します。 注意 「Blocked Status」は、運用上のステータスであり、設定されたステータスではありません。それは再起動後には保持されません。初期値では、ステータスは「Unblock」です。 CP の操作上のステータスが「Enabled」である時にだけ、「Block」と「Unblock」は使用できます。
Authenticated Users	このキャプティブポータルへの認証に成功し、現在ポータルを使用しているユーザ数を表示します。

「CP Activation and Activity」ページでは、以下のボタンが利用できます。

項目	説明
Block	「Block」をクリックすると、ユーザが、選択したキャプティブポータルを経由してネットワークへのアクセス権を取得することを防ぎます。
Unblock	選択したキャプティブポータルの「Blocked Status」が「Blocked」の場合、「Unblock」をクリックすると、キャプティブポータルを経由したネットワークへのアクセスを許可します。
Refresh	「Refresh」ボタンをクリックすると、画面を最新の情報に更新します。

インタフェースアクティベーションステータスの参照

「Interface Activation Status」ページではキャプティブポータルインスタンスに割り当てられたすべてのインタフェースの情報を表示します。プルダウンメニューを使用して、情報を参照するポータルまたはインタフェースを選択します。

WLAN タブ > Security > Captive Portal > Interface Status の順にメニューをクリックし、「Interface Activation Status」タブを参照します。

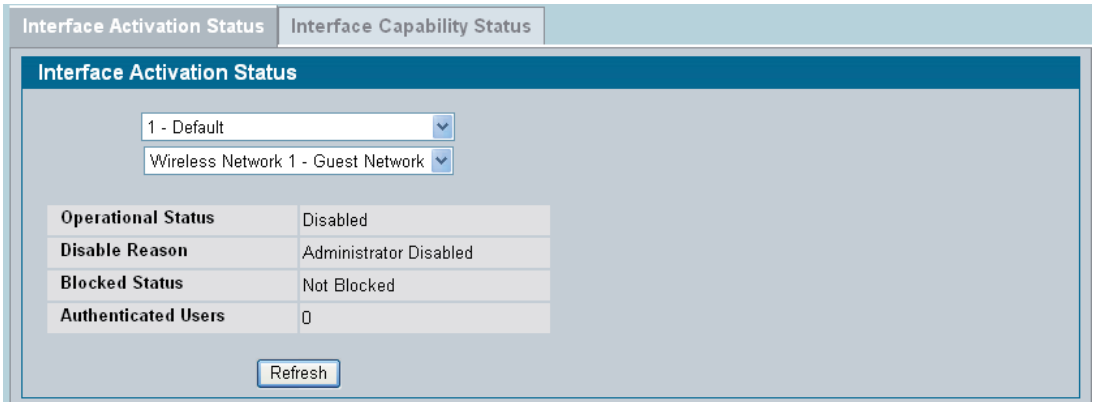


図 9-10　Interface Activation Status 画面

表 9-10 では「Interface Activation Status」ページ内の各項目について説明します。

表 9-9　Interface Activation Status

項目	説明
Operational Status	ポータルが指定インタフェースでアクティブであるか否かを表示します。
Disable Reason	選択した CP が本インタフェースで無効の場合、以下の原因から一つが表示されます。 • Interface Not Attached - インタフェースは割り当てされていません。 • Disabled by Administrator - 管理者が無効にしました。
Blocked Status	キャプティブポータルが一時的に認証に対してブロックされるかどうかを表示します。
Authenticated Users	本インタフェースにおけるキャプティブポータルインスタンスを使用して認証されているユーザ数を表示します。

Interface Capability Status の参照

「Interface Capability Status」ページには、割り当てられた CP を持つインタフェースに関する情報があります。また、さまざまな機能に関する情報もあります。本ページは、特に本インタフェースに接続するクライアントに対して CP 経由で提供するサービスを表示します。サービスのリストはインタフェースの能力によって決定されます。

WLAN タブ > Security > Captive Portal > Interface Status の順にメニューをクリックし、「Interface Capability Status」タブを参照します。

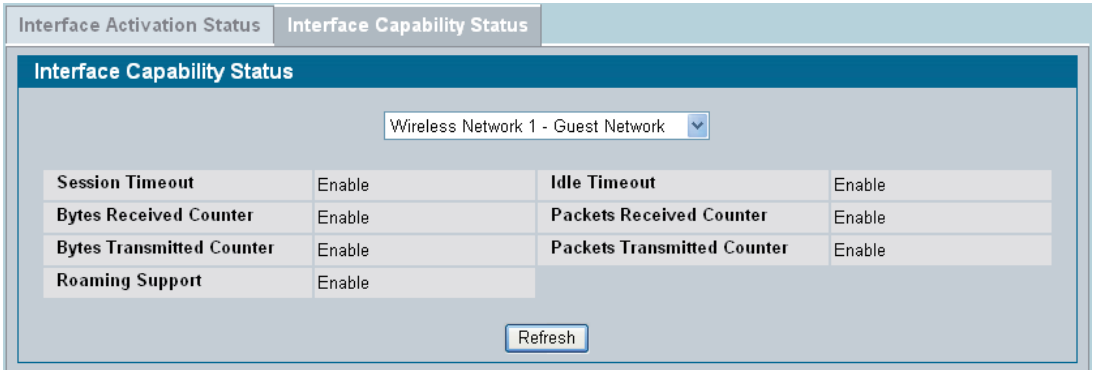


図 9-11　Interface Capability Status 画面

プルダウンメニューにはスイッチで利用可能なすべての物理的インタフェースおよび無線インタフェースがあります。物理的 (有線) インタフェースは、スロット番号、ポート番号およびインタフェースタイプを含むポート種別により識別されます。ポート種別にはスロット番号、ポート番号およびインタフェースタイプが含まれます。無線インタフェースは、無線ネットワーク番号と SSID により識別されます。プルダウンメニューを使用して、表示する情報を持つインタフェースを選択します。

表 9-11 では「Interface Capability Status」ページ内の各項目について説明します。

表 9-11　インタフェースと Capability Status

項目	説明
Session Timeout	インタフェースがクライアントセッションのタイムアウトをサポートするかどうかを表示します。本属性はすべてのインタフェースでサポートされます。
Bytes Received Counter	インタフェースが各クライアントから受信したバイト数の表示をサポートするかどうかを表示します。
Bytes Transmitted Counter	インタフェースが各クライアントに送信したバイト数の表示をサポートするかどうかを表示します。
Roaming Support	インタフェースがクライアントのローミングをサポートするかどうかを表示します。無線インタフェースだけがクライアントローミングをサポートします。
Idle Timeout	ユーザが何もトラフィックを送信または受信しない場合のタイムアウトをインタフェースがサポートするかどうかを表示します。
Packets Received Counter	インタフェースが各クライアントから受信したパケット数の表示をサポートするかどうかを表示します。
Packets Transmitted Counter	インタフェースが各クライアントに送信したパケット数の表示をサポートするかどうかを表示します。

9.6 クライアントサマリの参照

キャプティブポータルを経由して D-Link 統合アクセスシステムに接続する無線クライアントに関する情報を参照します。

WLAN タブ > Security > Captive Portal > Client Connection Status の順にメニューをクリックします。

クライアントに関するサマリ情報の参照

「Client Summary」ページを使用して、キャプティブポータル経由でネットワークに接続するすべての認証無線クライアントに関するサマリ情報を参照します。本ページから、キャプティブポータルに 1 つ以上の認証クライアントを手動で強制的に切断させることができます。無線クライアントのリストはクライアント MAC アドレスによってソートされます。

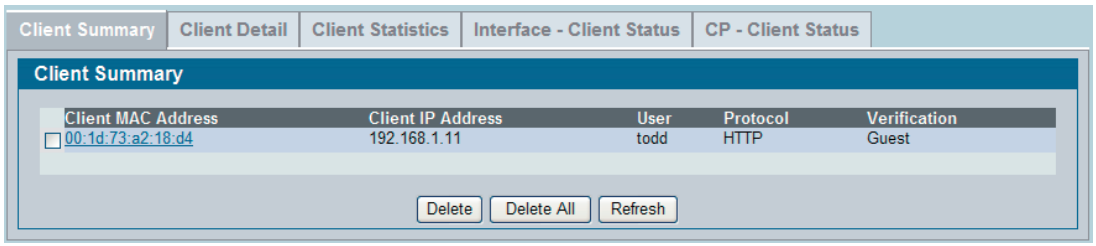


図 9-12　Client Summary 画面

表 9-12 は「CP Summary」ページの各項目を説明します。

表 9-12　Client Summary

項目	説明
Client MAC Address	キャプティブポータル経由でネットワークに接続するクライアントの MAC アドレスを示します。
Client IP Address	クライアントの IP アドレスを示します。
User	接続するクライアントのユーザ名（またはゲスト ID）を表示します。
Protocol	現在の接続プロトコル（HTTP または HTTPS）を表示します。
Verification	現在のアカウントタイプ（Guest、Local または RADIUS）を表示します。

キャプティブポータルが認証クライアントを切断するためには、そのクライアントの MAC アドレスの左側にあるチェックボックスを選択して「Delete」ボタンをクリックします。すべてのキャプティブポータルからすべてのクライアントを切り離すためには、「Delete All」ボタンをクリックします。

クライアントの MAC アドレスをクリックすると、追加のステータス情報を表示できます。

クライアント詳細情報の参照

「Client Status」ページでは、キャプティブポータル経由でネットワークに接続する各クライアントの詳細情報を表示します。

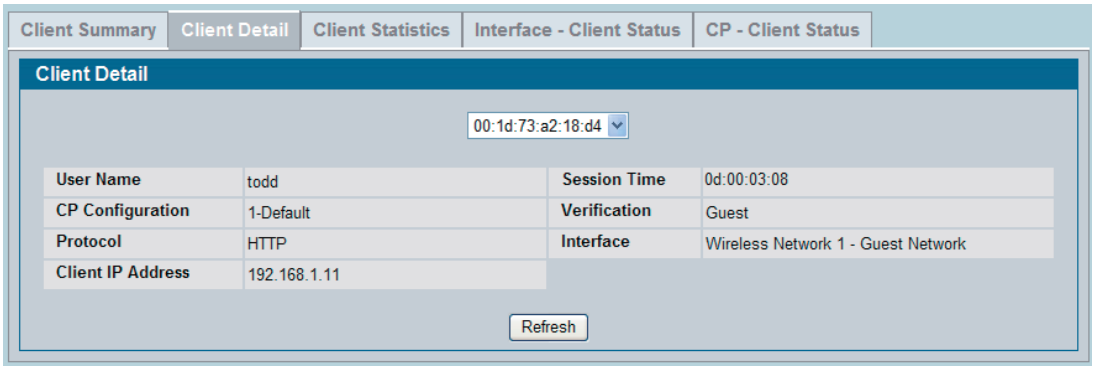


図 9-13　Client Detail 画面

プルダウンメニューは MAC アドレスごとに各関連するクライアントを表示します。クライアントに関するステータス情報を参照するためには、リストから選択します。

表 9-13 は「Client Detail」ページの各項目を説明します。

表 9-13　Client Detail

項目	説明
User Name	接続するクライアントのユーザ名（またはゲスト ID）を表示します。
CP Configuration	クライアントが使用している CP 名を表示します。スイッチは 10 個の CP をサポートしています。
Protocol	現在の接続プロトコル（HTTP または HTTPS）を表示します。
Client IP Address	クライアントの IP アドレスを表示します。
Session Time	クライアントが認証されてから経過した時間を表示します。
Verification	現在のアカウントタイプ（Guest、Local または RADIUS）を表示します。
Interface	クライアントが使用しているインタフェースを表示します。

クライアント統計情報の参照

「Client Statistics」ページを使用して、クライアントが送信または受信したトラフィックに関する情報を参照します。

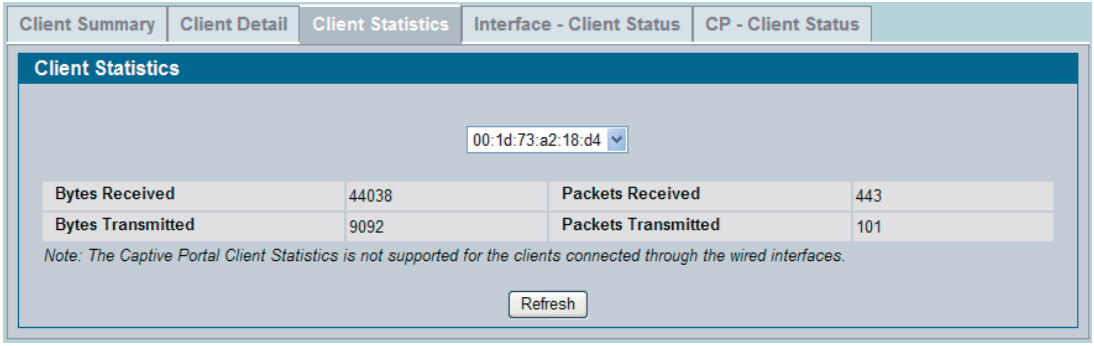


図 9-14　Client Statistics 画面

プルダウンメニューは MAC アドレスを使用して各関連クライアントを表示します。クライアントに関する統計情報を参照するために、リストから選択します。

表 9-14 では「Client Statistics」ページの各項目を説明します。

表 9-14　クライアントインタフェース関連の接続統計情報

項目	説明
Bytes Transmitted	クライアントが送信した合計バイト数。
Bytes Received	クライアントが受信した合計バイト数。
Packets Transmitted	クライアントが送信した合計パケット数。
Packets Received	クライアントが受信した合計パケット数。

クライアントインタフェース関連ステータスの参照

「Interface - Client Status」ページを使用して、指定インタフェースに認証されているクライアントを参照します。

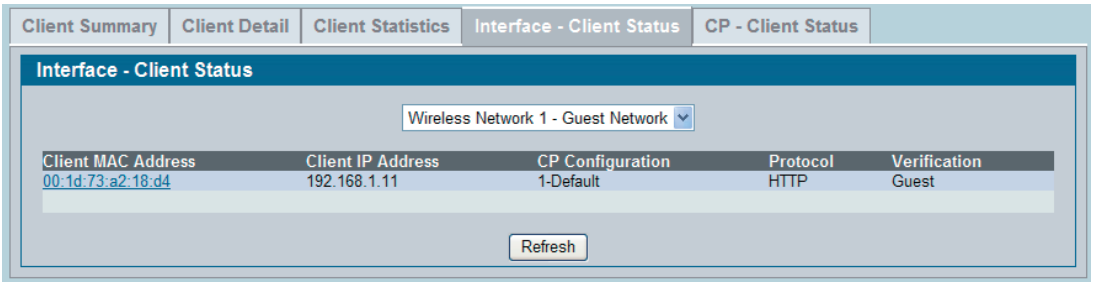


図 9-15　Interface - Client Status 画面

表 9-15 では「Interface - Client Status」ページ内の各項目について説明します。

表 9-15　Interface - Client Status

項目	説明
Client MAC Address	無線クライアントの MAC アドレスを示します。
Client IP Address	無線クライアントの IP アドレスを示します。
CP Configuration	クライアントがネットワークにアクセスするために使用したキャプティブポータルを示します。
Protocol	現在の接続プロトコル（HTTP または HTTPS）を表示します。
Verification	現在のアカウントタイプ（Guest、Local または RADIUS）を表示します。

Client CP Association Status の参照

「CP - Client Status」ページを使用して指定 CP 設定に認証されているクライアントを参照します。

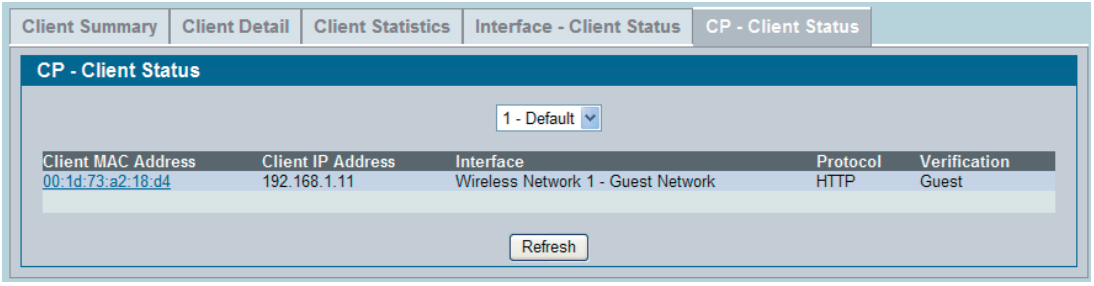


図 9-16　CP - Client Status 画面

プルダウンメニューはスイッチに設定されている各 CP を表示します。CP に接続するクライアントに関する情報を参照するためには、リストからそれを選択します。

表 9-16 では「Client CP Association Status」ページ内の各項目について説明します。

表 9-16　CP - Client Status

項目	説明
Client MAC Address	無線クライアントの MAC アドレスを示します。
Client IP Address	無線クライアントの IP アドレスを示します。
Interface	クライアントがネットワークにアクセスするために使用したインタフェースを示します。
Protocol	現在の接続プロトコル（HTTP または HTTPS）を表示します。
Verification	現在のアカウントタイプ（Guest、Local または RADIUS）を表示します。

9.7 SNMP トラップ設定

「SNMP Trap Configuration」ページを使用して、SNMP トラップをキャプティブポータルから送信するかどうかを設定し、トラップを生成するキャプティブポータルのイベントを指定します。

すべての CP SNMP トラップは初期値では無効に設定されています。

各種のキャプティブポータル機能に SNMP トラップ設定を行うためには、**WLAN タブ > Security > Captive Portal > SNMP Trap Configuration** の順にメニューをクリックします。

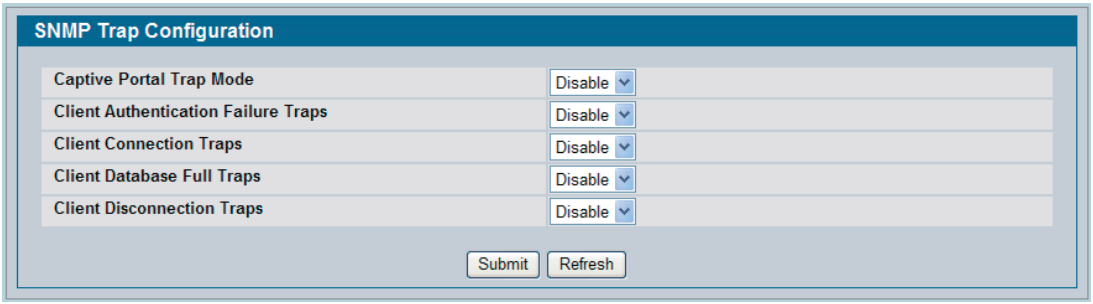


図 9-17　SNMP Trap Configuration 画面

表 9-17 では、ステータスが有効された際に SNMP トラップを生成するイベントについて説明します。

表 9-17　SNMP Trap Configuration

項目	説明
Captive Portal Trap Mode	以下のキャプティブポータルのトラップモードから 1 つを選択します。 • Enable - スイッチの SNMP エージェントは有効とされているキャプティブポータルの SNMP トラップを生成します。 • Disable - スイッチの SNMP エージェントは、それらが個別に有効とされていてもキャプティブポータルの SNMP トラップは生成されません。
Client Authentication Failure Traps	有効にすると、クライアントがキャプティブポータルに認証を試みて失敗した場合、SNMP エージェントがトラップを送信します。
Client Connection Traps	有効にすると、クライアントが認証され、キャプティブポータルに接続した場合、SNMP エージェントがトラップを送信します。
Client Database Full Traps	有効にすると、エントリがフル状態のクライアントデータベースに追加されなかった場合に SNMP エージェントがトラップを送信します。
Client Disconnection Traps	有効にすると、クライアントがキャプティブポータルから切断された場合、SNMP エージェントがトラップを送信します。

第 10 章　無線ネットワークの視覚化

WLAN 視覚化コンポーネントは無線ネットワークの情報を図式化して表示するためのオプション機能です。本機能では Java アプレットを使用して、D-Link 統合スイッチ、D-Link アクセスポイント、他社のアクセスポイント、および接続する無線クライアントを表示します。本機能によって、建物の中でのデバイスの位置等をビジュアル化して確認できます。

まず、用意したカスタムイメージをアップロードして図の背景を作成します。そして、スイッチにより検出された WLAN を構成するデバイスを図中に配置し、ご使用の無線ネットワークをリアルに表現します。視覚化された WLAN 図上の各デバイスから、そのデバイスについての情報を取得したり、Web インタフェースの設定ページへリンクすることもできます。

本章は以下の項で構成され、D-Link 統合アクセスシステムの WLAN 視覚化コンポーネントの操作、管理方法について説明します。

項目	説明	参照ページ
背景画像のインポートと設定	WLAN 視覚化グラフ用画像をアップロードします。	131 ページ
グラフコンポーネントの設定	WLAN 視覚化アプリケーションを使用して、画像をグラフに割り付けます。	131 ページ
メニューバーについて	WLAN 視覚化ツールで使用できるメニューについて説明します。	134 ページ
グラフの管理	グラフにコンポーネントを配置後の情報の取得、グラフからの削除、またはそれらの管理やモニタを行います。	136 ページ

図 10-1 に 2 台のアクセスポイントを管理する D-Link 統合スイッチが配置されているフロアプランの例を示します。図中には 2 台のスイッチと不正アクセスポイントも表示されています。

図 10-1　WLAN の視覚化例

10.1 背景画像のインポートと設定

初期状態では、WLAN 視覚化グラフ（図）に背景画像は設定されていません。例えば、オフィスの見取り図など、1 つまたは複数の画像をアップロードして、サイトの状況や、サイトに関係した情報をグラフを提供します。

アップロードする画像のフォーマットは、以下の通りです。

- GIF（Graphics Interchange Format）
- JPG（Joint Photographic Experts Group）

また、WLAN コンポーネントがグラフ内で目立たなくなるため、カラー画像をご使用にならないことをお勧めします。

以下の手順で、WLAN 視覚化グラフに使用する画像をスイッチにアップロードしてください。

1. **WLAN タブ > WLAN Visualization > Download Image** をクリックします。
2. 「参照」ボタンをクリックしてファイルの場所を検索します。
3. アップロードするファイルを選択して「Start File Transfer」ボタンをクリックします。

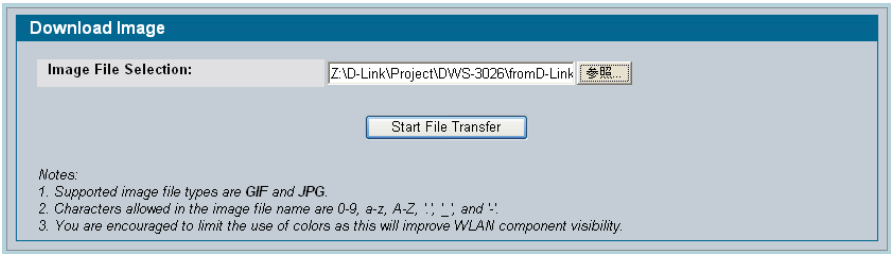


図 10-2　ダウンロードファイルの指定

画像ファイルをアップロードして現在の設定を保存すると、その画像はスイッチに登録されます。その後 WLAN 視覚化アプリケーションを使用して、グラフに割り付けることができるようになります。

10.2 グラフコンポーネントの設定

WLAN 視覚化ツールを起動するためには、**WLAN タブ > WLAN Visualization > Launch...** をクリックします。新しいブラウザの画面が表示され、Java アプレットが起動します。

初めて WLAN 視覚化ツールを起動する場合、背景画像が表示されません。また、検出された WLAN コンポーネントは図示されません。画面は 2 つの区画で構成されています。左側の区画は、さらに 3 つに分割されており、図示されていないコンポーネントが表示されます。右側の区画は、定義した図が表示されるエリアです。この図表示エリアは、初めは空白になっています。WLAN コンポーネントを取り込む前に、このエリアに背景を取り込んでおきます。

新規グラフの作成

新規にグラフ（図）を作成し、背景画像をアップロードするためには、WLAN 視覚化ツールを起動して以下の手順を実行してください。

1. 「WLAN Visualization」メニューバーの「Edit」で「New Graph...」を選択し、「New Graph Definition」ダイアログボックスを表示します。

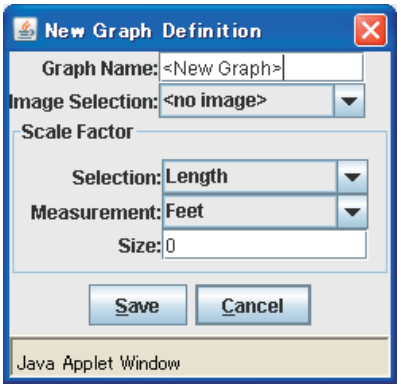


図 10-3　画像の選択と寸法の指定

2. グラフを識別する名前を入力し、背景として使用する画像を選択します。画像をグラフの背景として使用する方法については、131 ページの「10.1 背景画像のインポートと設定」を参照してください。

3. インポートする背景画像の大きさ（高さまたは幅）を示す、サイトでの実際の寸法を指定します。
「Selection」と「Measurement」プルダウンメニューから、指定した寸法を「Height（高さ）」または「Width（幅）」から、さらに単位を「メートル」または「フィート」から選択します。

ここで指定する値により背景画像の縮尺が決定されます。そしてこの縮尺値により、WLAN 視覚化ツールによるアクセスポイントの RF カバー範囲の見え方が変わってきます。そのため正確な寸法を入力する必要があります。

例えば、次のページの 2 つの図では、同じ背景画像を使用し、アクセスポイントも同じ位置に配置しています。一つ異なるのは、片方のグラフでは図の高さが 200 フィートと指定しているのに対して、もう片方では 800 フィートと指定しています。

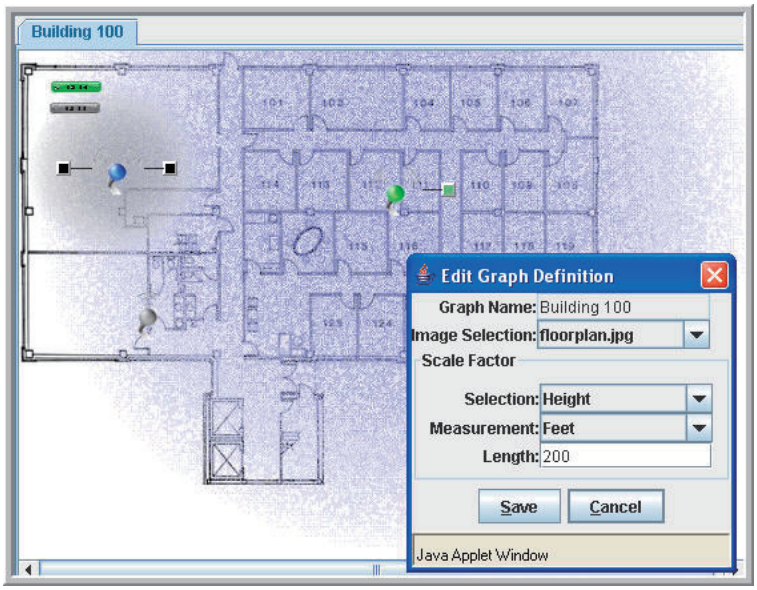


図 10-4　高さを 200 フィートにしたグラフ

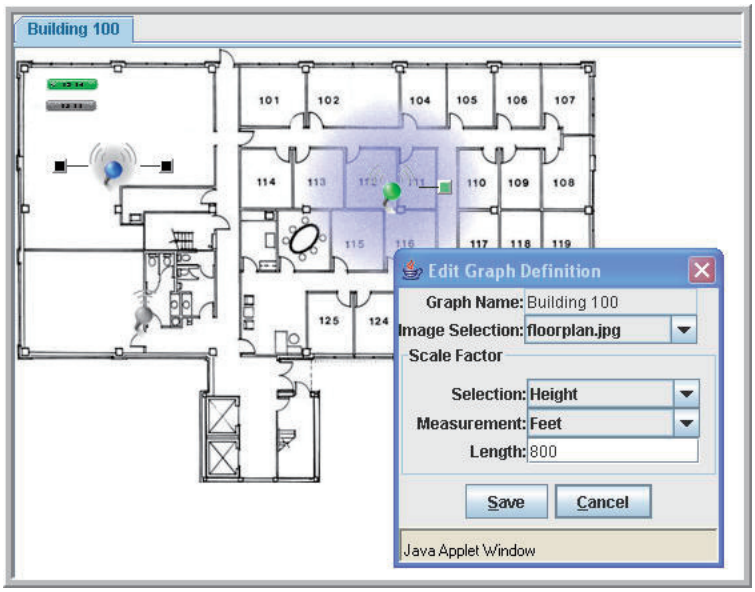


図 10-5　高さ =800 フィートにしたグラフ

4. 「Save」ボタンをクリックして、グラフの設定を完了させます。
スイッチにアップロードした背景画像が、グラフの背景画像として表示されます。

本ツールでは、複数のグラフの作成も可能です。例えば、ご使用のネットワークが複数階のフロアにまたがっている場合は、各階ごとにグラフを作成することができます。追加したグラフは、図 10-6 で示すように、グラフ上部にタブの形で表示されます。

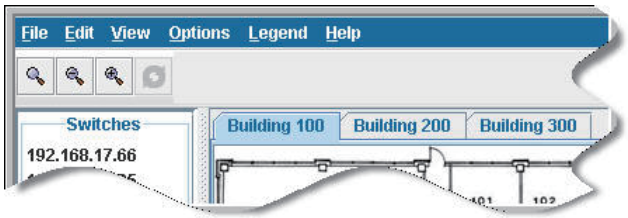


図 10-6　複数のグラフの場合

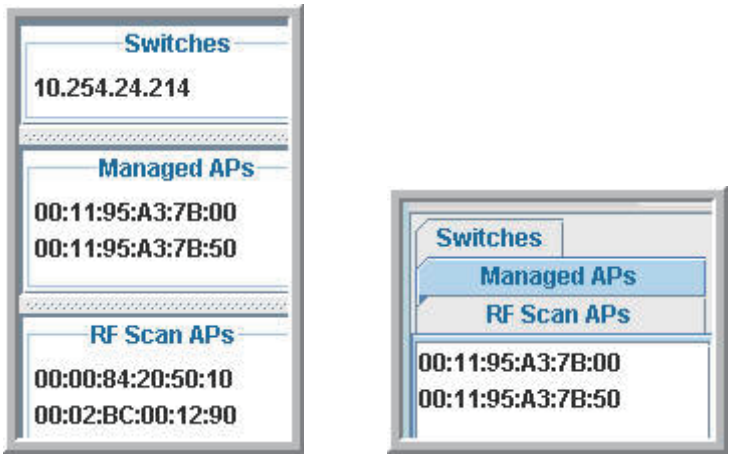
グラフの追加は、本項の手順を繰り返して行います。

WLAN コンポーネントの図示化

WLAN 視覚化ツールでは、スイッチが検出した WLAN コンポーネントを自動的に表示します。
画面上には、以下の種類のコンポーネントが表示されます。

- スイッチ（統合スイッチおよびピアスイッチ）
- 管理対象アクセスポイント
- RF スキャンアクセスポイント

これらのコンポーネントは、グラフ上にドラッグされるまでは、画面左の区画に表示されています。「View」メニューから、コンポーネントを「リスト表示（上記 3 種類がすべて表示されているタイプ）」または「タブ表示（1 種類のみの表示で残りはタブにまとめられているタイプ）」のいずれかを選択することができます。図 10-7 に同じ内容のコンポーネント群の「リスト表示」と「タブ表示」の例を示します。アクセスポイントについてはその場所名、または MAC アドレスが表示され、スイッチについてはその IP アドレスが表示されます。



リスト表示　　タブ表示

図 10-7　リスト表示とタブ表示

無線クライアントは、左側の区画には表示されず、図示化された D-Link アクセスポイントとの接続が検出されると、自動的にグラフエリアに表示されます。

図示化されていないコンポーネント上にマウスをポイントすると、図 10-8 で示すように、そのコンポーネントに関する詳細情報がポップアップ表示されます。

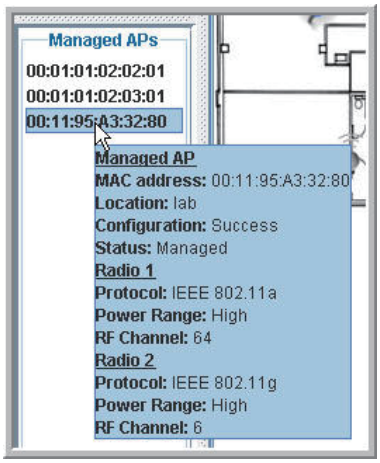


図 10-8　　コンポーネント情報ポップアップ表示

左区画にリスト表示されているコンポーネントを図示化するためには、そのコンポーネントを選択し、そのままグラフエリア内にドラッグします。サイト内でコンポーネントが実際に配置されている場所を示すグラフエリア内の位置までドラッグしたら、マウスから手を離します。
スイッチまたはアクセスポイントをグラフエリアに移動させると、そのコンポーネントは左区画のリスト表示から削除されます。

「Shift」キーまたは「Ctrl」キーを押下しながら、コンポーネントを選択すると複数選択が可能になります。複数選択したもののうちのどれか 1 つの上で右クリックをすると、選択したものすべてを一括してグラフエリア内へドラッグすることができます。

図 10-9　グラフ化されたコンポーネント

グラフからコンポーネントを削除するためには、コンポーネント上で右クリックし、「Edit」から「Un-Graph」を選択します。

10.3 メニューバーについて

以下の表では、WLAN 視覚化ツールで使用できるメニューの概要を示します。

表 10-1　WLAN 視覚化ツールのメニューバー

メニュー項目		説明
File	Force refresh	手動更新。Java クライアントアプリケーションの再同期します。グラフの編集後、本メニューを実行して、画面を更新します。
	Reconnect and Refresh	クライアントアプリケーションを一旦スイッチから切断して、再接続します。
	Exit	WLAN 視覚化アプリケーションを終了します。
Edit	New Graph	新規のグラフを作成し、グラフ名、背景画像、縮尺を設定するための画面を開きます。
	Edit Graph	作成済みのグラフを開きます。背景画像と縮尺は変更可能ですが、グラフ名を変更するためには、新規のグラフを作成する必要があります。
	Delete Graph	作成済みのグラフを削除します。本項目を選択すると、本当に削除を実行するかどうか確認するダイアログボックスが表示されます。
	Image Management	使用可能な背景画像のリストを表示します。また画像の削除も本項目から行います。
View	Ungraphed Components	左区画の図示化されていないコンポーネント群の表示方法を選択します。 • Tab View - 1 種類のコンポーネントのみを表示し、他の種類をタブにまとめて表示します。 • List View - すべての種類のコンポーネントを表示します。 109 ページの図 10-9 に上記の 2 種類の表示方法の違いを示しています。

メニュー項目		説明
	AP Power Display	アクセスポイントの出力エリアイメージを選択します。 • Disable Power Display - 出力エリアイメージの表示を行いません。 • Show 802.11a - 802.11a モードで動作している無線インタフェースの出力エリアイメージを表示します。 • Show 802.11b/g - 802.11b/g モードで動作している無線インタフェースの出力エリアイメージを表示します。 出力エリアイメージのサイズは、無線インタフェースの送信電力に基づき、3 種類（低、中、高）のが用意されています。またそのサイズは現在使用している背景画像の倍率にも依存します。 1 つのモードがアクセスポイントの 2 つの無線インタフェースに設定されている場合は、2 つの出力エリアイメージが表示されます。 **注意** 出力エリアイメージの色は、接続に使用するチャンネルによって異なります。 もし、2 台のアクセスポイントが、お互いの伝送範囲内において同じチャンネル（または近隣のチャンネル）を使用していれば、アクセスポイント同士が干渉し合い、無線クライアントの通信品質は悪くなります。そのような干渉を防ぐために、以下のいずれかを実行してください。 • アクセスポイントの送信電力を低く設定する • アクセスポイント同士を物理的に離して設置する • アクセスポイント上で自動チャンネル調整アルゴリズムを使用する。または干渉を起こさないように手動でチャンネルを調整する。 **警告** 出力エリアイメージは例示を目的としており、あくまでもイメージです。実際の電力分布は、オフィスの壁などの伝播特性やバックグラウンドの RF ノイズなどにより異なります。
Options	Show Managed APs	グラフ上での D-Link アクセスポイントの表示を指定します。チェックボックスのチェックを外すと、アクセスポイントは見えなくなりますが、アイコン化したオブジェクト自体は記憶されています（左区画は戻りません）。
	Show RF Scan APs	グラフ上に RF スキャンにより検出されたアクセスポイントを表示するかどうかを指定します。チェックボックスのチェックを外すと、アクセスポイントは見えなくなりますが、アイコン化したオブジェクト自体は記憶されています。
	Show Managed AP Clients	グラフ上にアクセスポイントと接続中のクライアントを表示するかどうかを指定します。チェックボックスのチェックを外すと、クライアントは見えなくなりますが、アイコン化したオブジェクト自体は記憶されています。
Legend	Images	WLAN コンポーネントとアイコンの対応を表示します。
	Channel Color	伝送に使用されているチャンネルと、出力エリアイメージで使用する色の対応を表示します。
Help	WLAN Visualization	新しい HTML 画面を表示し、WLAN オンラインヘルプを表示します

「Legend」メニューについて

「Legend（凡例）」メニューを選択すると、グラフ上に表示されるアイコンと、それらの色についての情報を確認することができます。
「Images」を選択すると、グラフ上で各 WLAN コンポーネントを表すアイコンを表示します。

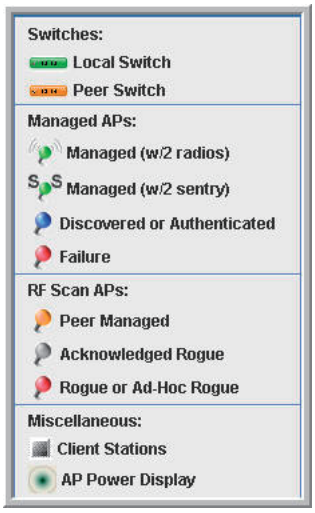


図 10-10　アイコンの凡例

凡例が示すように、スイッチ配下のアクセスポイントは、その状態によって青、緑または赤で表示されます。

- 青 - アクセスポイントはスイッチにより検出されましたが、状態遷移中です。アクセスポイントは認証待ちであるか、または認可・認証はされたが設定がなされていない状態です。
- 緑 - AP プロファイルが適用されており、管理対象モードで動作中です。
- 赤 - スイッチとの通信が切断されました。アクセスポイントが再起動中であるか、または認証に失敗しました。

「Sentry」モードでの動作中は、図 10-11 で示すように、アクセスポイントのアイコンのアンテナが「S」という文字に変わって表示されます。

図 10-11 「Sentry」モード - 詳細図

「Sentry」モード中は、アクセスポイント周囲の出力イメージはグレーで表示されます。
チャンネルカラーの凡例では、出力イメージと各チャンネルを表す色の対応を示します。無線インタフェースが通信に使用している各チャンネルはそれぞれ色が割り当てられています。利用できるチャンネルは、無線モードおよび国によって異なります。

図 10-12 チャンネルの色

使用中のチャンネルを表示するためには、管理対象のアクセスポイント上にマウスをポイントして、ポップアップ画面を表示させます。画面中に使用中のチャンネルを含む、アクセスポイントの諸情報が確認できます。

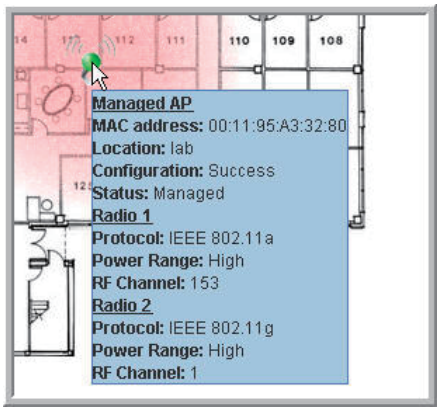


図 10-13 アクセスポイント情報ポップアップ画面

各オブジェクト上で右クリックすることにより、さらに詳細な情報を確認できます。この機能については、次の節で説明します。

10.4 グラフの管理

グラフにコンポーネントを配置後、コンポーネント上で右クリックすることにより、そのコンポーネントについてのさらに詳細な情報の取得や、グラフからの削除、または Web インタフェースのページに遷移して、コンポーネントの管理やモニタを行うことができます。

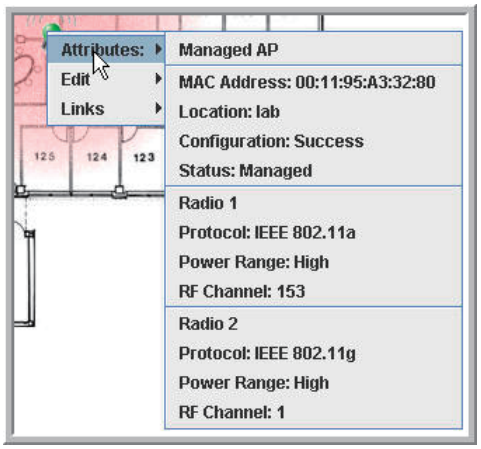


図 10-14 無線コンポーネントの属性表示

表 10-4 に各コンポーネントについて、表示できる属性および Web インタフェースのコマンドへのリンクを示します。

表 10-4　コンポーネント情報

コンポーネント	属性	リンク / コマンド
スイッチ	IP Address	Basic Setup（基本設定） RF Management（RF 管理） Global Status/Statistics（グローバル状態 / 統計情報）
ピアスイッチ	IP Address	Peer Switch Status（ピアスイッチ状態）
管理対象 AP	MAC Address（MAC アドレス） Location（場所） Configuration（設定） Status（状態） Radio（管理対象 無線インタフェース - 1 または 2） Protocol（プロトコル - IEEE 802.11b/g または 802.11a） Power Range（出力エリア - 低 / 中 / 高） RF Channel（RF チャンネル - チャンネルプラン Sentry モード（有効な場合）によって異なります。）	Configuration（設定） • AP Profile Configuration（AP プロファイル設定） • Valid AP Configuration（Valid AP 設定） Management（管理） • Radio（無線） • Software Download（ソフトウェアダウンロード） • Debug（デバッグ） Status and Statistics（状態と統計） • Managed AP Status Detail（管理対象 AP 詳細状況） • Radio Status and Statistics（無線状態と統計） コマンド : AP Reset（AP リセット）
他アクセスポイント	MAC Address（MAC アドレス） Status（状態） - Rogue、Peer Managed、Acknowledged AP（不正、ピア管理下または認識済み AP） RF チャンネル	Status（状態） コマンド • Manage RF Channel（管理対象化） • Acknowledge（認識）
無線クライアント	MAC Address（MAC アドレス） Radio（無線インタフェース - 1 または 2） RF Channel（RF チャンネル - チャンネルプランによって異なります。）	Associated Client Status Detail（接続中のクライアント詳細状況） コマンド : Disassociate（切断）

付録 A　D-Link 統合アクセスシステムの初期設定

本章では、D-Link 統合スイッチ用設定の初期値、およびスイッチがアクセスポイントを検出・認証後に適用するデフォルト AP プロファイルに設定されている値を示します。

A.1 DWS-3026 の初期設定

表 A-1 は、DWS-3026 初期設定を示します。

表 A-1　スイッチの初期設定

設定項目		初期値
システム情報	ユーザ名	admin
	Password	None
ネットワーク情報	DHCP クライアント	無効
	ネットワークコンフィグレーションプロトコル	なし
	IP アドレス	10.90.90.90
	サブネットマスク	255.0.0.0
	802.1Q	有効
	管理用 VLAN ID	1
	タグなし VLAN ID	1
	スパニングツリープロトコル	有効
WLAN 情報	無線スイッチモード	有効
	AP 認証	無効
	AP 認知	ローカル
	国コード	US
	デフォルトプロファイル名	Default
	ピアスイッチグループ ID	1
	L2（VLAN）/L3（IP）検出	有効
	SNMP トラップ	無効
	Client Roam Timeout	30 秒
	Ad Hoc Client Status	24 時間
	AP Failure Status	24 時間
	Client Failure Status	24 時間
	RF Scan Status	24 時間

A.2 D-Link アクセスポイントプロファイルの初期設定

表 A-2 はデフォルト AP プロファイルの設定内容を示します。初期設定では、D-Link アクセスポイントがスイッチと接続する時、アクセスポイントが認知されると同時に本表中の設定内容が適用されます。

表 A-2　デフォルト AP プロファイル設定

	設定項目	初期値
システム情報	ユーザ名	admin
	パスワード	admin
ネットワーク情報	DHCP クライアント	有効
	管理用 IP アドレス	10.90.90.91（DHCP による割り当てがない場合）
	サブネットマスク	255.0.0.0（DHCP による割り当てがない場合）
	管理用 VLAN ID	1
	タグなし VLAN ID	1
無線設定	無線インタフェース（1 と 2）	On
	無線 1 IEEE 802.11 モード	802.11b/g
	無線 2 IEEE 802.11 モード	802.11a **注意** アクセスポイントが 802.11a をサポートしない規制範囲で動作する場合、この無線インタフェースは無効になり、いずれのモードもサポートしません。
	RF Scan Other Channels	有効
	RF Scan Interval	60 秒
	RF Scan Duration	10 ミリ秒
	Super AG	無効
	Extended Range	無効
	Automatic Channel	有効
	Automatic Power	有効
	Initial Power	100
	Load Balancing	無効
	Load Utilization	60%
	Maximum Clients	256
	RTS Threshold	2347 バイト
	DTIM Period	10 ビーコン
	Fragmentation Threshold	2346 バイト
	Beacon Period	100 ミリ秒
	Rate Limiting	無効
	Rate Limit	50 パケット / 秒
	Rate Limit Burst	75 パケット / 秒
	Rate Sets Supported(Mbps)	IEEE 802.1a: 54,48,36,24,18,12,9,6 IEEE 802.1g: 54,48,36,24,18,12,11,9,6,5.5,2,1 IEEE 802.1b: 11,5.5,2,1 Atheros Turbo 5 GHz: 108,96,72,48,36,24,18,12
	Rate Sets(Mbps) (Basic/Advertised)	IEEE 802.1a: 24,12,6 IEEE 802.1g: 11,5.5,2,1 IEEE 802.1b: 2,1 Atheros Turbo 5 GHz: 48,24,12
仮想アクセスポイントとネットワーク設定	Status	双方の無線インタフェースにおいて VAP0 が有効。他の VAP は無効。
	Network 名 (SSID)	Guest Network (VAP0)
	VLAN	1
	Hide SSID	無効
	L3 Tunnel	無効
	Security Mode	Open System
	Ignore Broadcast	無効
	MAC Authentication	無効
	RADIUS IP Address	プロファイル使用 (Global)
	RADIUS Accounting	無効
その他の設定	QoS	有効
	WMM	有効

A.3 キャプティブポータル設定の初期値

表 A-3 はキャプティブポータル設定の初期値を示します。

表 A-3　キャプティブポータル設定の初期値

設定項目		初期値
Global Configuration	Operational Status	Enabled
	Additional HTTP Port	None
	Peer Switch Statistics Reporting Interval	120 seconds
	Authentication Session Timeout	600 seconds
CP Configuration	Status	Enabled
	Configuration Name	None
	Protocol Mode	HTTP
	Verification Mode	Guest
	User Group	None
	URL Redirect Mode	Disabled
	Session Timeout	0 (unlimited)
	Idle Timeout	0 (unlimited)
	Languages	English

付録 B　外部 RADIUS サーバの設定

Valid AP コンフィグレーションは D-Link 統合スイッチのローカルデータベース内、または外部 RADIUS サーバ内に保存することができます。ここでは、RADIUS サーバ内にコンフィグレーション設定を行うために定義する属性について説明します。

RADIUS サーバにアクセスポイントの情報を設定し、1 台の RADIUS サーバに各ピアスイッチが情報を取得するようにすると、それぞれのスイッチに分散して設定するよりも、はるかに効率化が図れます。

B.1 RADIUS サーバでのアクセスポイント設定

アクセスポイントは物理 MAC アドレスによって識別されるため、各アクセスポイントについて MAC アドレスとユーザ名を RADIUS サーバに登録する必要があります。表 B-1 に RADIUS サーバに登録する各アクセスポイントの属性を示します。D-Link ベンダ ID「6132」を入力し、属性名の前に、識別子「D-Link-Wireless-AP-*」（* には属性名が続きます）を付加して、ベンダ固有属性の登録を行ってください。

注意 本付録の記述は、802.1X を使用したアクセスポイントのネットワーク認証用の設定を含みません。802.1X 認証は Valid AP コンフィグレーションとは別の機能となっています。ネットワーク認証は、アクセスポイントに接続するエッジデバイス（D-Link 統合スイッチとは限りません）により行われます。

表 B-1　アクセスポイント用 RADIUS 属性

RADIUS サーバ属性	説明	値の範囲	必須 / 任意
User-Name(1)	アクセスポイントの MAC アドレス	有効 MAC アドレス	必須
User-Password(2)	AP エントリ検索に使用するパスワード	8-63 文字の英数字。 初期値は「NOPASSWORD」。	必須
Vendor-Specific(26) Location	アクセスポイントの場所	1-32 文字の半角英数字	任意
Vendor-Specific(26) Mode	本アクセスポイントがスイッチまたは管理者の管理下にあるか、または不正 AP であるかを示します。	WS Managed(1) Standalone (2) Acknowledged Rogue(3)	必須
Vendor-Specific(26) Profile-ID	アクセスポイントがスイッチの管理下にある時の、本アクセスポイント用のコンフィグレーションプロファイルの ID。	1-16	上記「Mode」が「WS Managed」である時必須。
Vendor-Specific(26) Switch-IP	本 RADIUS サーバを複数台のスイッチで共有している場合に、本アクセスポイントを管理するスイッチの IP アドレス。	有効 IP アドレス	任意
Vendor-Specific(26) Radio-1-Chan Vendor-Specific(26) Radio-2-Chan	無線インタフェースの固定チャンネル。	有効なチャンネルは、規制範囲（国コード）および、AP プロファイルにおいて、そのインタフェースに設定した無線モードにより異なります。 選択したチャンネルが有効でない場合は、無視されます。「0」は自動チャンネル割り当てを示します。	任意。 定義されたチャンネルが有効であるならば、自動チャンネル割り当てによる設定は上書きされます。
Vendor-Specific(26) Radio-1-Power	0,1-100 percent	0 は自動送信電力調整を示します。	任意。 定義された値が有効であれば自動送信電力調整による設定は上書きされます。
Vendor-Specific(26) Radio-2-Power	0,1-100 percent	0 は自動送信電力調整を示します。	任意。 定義された値が有効であれば自動送信電力調整による設定は上書きされます。

アクセスポイントと RADIUS サーバ間の認証が必要でない場合は、スイッチはスイッチ上の RADIUS クライアントと RADIUS サーバとの間の通信に「NOPASSWORD」というパスワードを使用します。スイッチ上の RADIUS クライアントはサーバからのエントリを読み出す際にこのパスワードを使用します。アクセスポイントの認証が必要な場合は、アクセスポイントからスイッチへの認証用（アクセスポイントからネットワークへの認証とは異なります）のパスワードの入力が必要になります。

B.2 FreeRADIUS を使用した RADIUS サーバ設定例

FreeRADIUS はオープンソースの RADIUS サーバで、http://www.freeradius.org から無料でダウンロードすることができます。本項では、RADIUS サーバを使用して D-Link 統合スイッチと D-Link アクセスポイントを認証するために必要なファイルの設定方法と、RADIUS データベース内での Valid AP 設定方法について説明します。

RADIUS クライアントの設定

RADIUS サーバを使用して、D-Link 統合スイッチまたは D-Link アクセスポイントを認証するためには、RADIUS サーバの etc/raddb/clients.conf ファイルに、それらデバイスのクライアントエントリの設定を行う必要があります。

エントリはクライアントの IP アドレス、共通鍵およびデバイスのニックネーム（または DNS 名）を含みます。

以下の情報を持つスイッチについて、clients.conf 内のエントリ設定例を示します。

- IP アドレス : 192.168.30.249
- サブネットマスク : 255.255.255.0
- 共通鍵 : wireless
- DNS 名 : wireless-sw1

以下のコードは clients.conf 内のクライアントエントリのフォーマットです。

```
client 192.168.30.249/24{
secret=wireless
shortname=wireless-sw1
}
```

属性辞書の作成と組み込み

属性辞書を作成すると、RADIUS サーバ上の Valid AP データベース内にアクセスポイントを登録する際に、属性と値を適用することができます。例えば、アクセスポイントの場所を指定する場合、定義する属性のフォーマットは以下のようになります。

```
ATTRIBUTE D-Link-Wireless-AP-Location    101     string  D-Link
```

ATTRIBUTE（属性）の各項目は以下の通りです。

- Attribute - エントリの種類。
- D-Link-Wireless-AP-Location - 属性名。
- 101 - 属性番号。場所を設定する際には本番号を指定します。
- string - 属性のデータの種類。
- D-Link - ベンダ固有の属性名。

以下の VALUE（値）欄では、アクセスポイントに指定することのできる AP モードの値を定義しています。

```
VALUE D-Link-Wireless-AP-Mode        WS-Managed          1
```

VALUE の各項目は以下の通りです。

- VALUE - エントリの種類。
- D-Link-Wireless-AP-Mode - 属性名。
- WS-Managed - 属性に対する値。
- 1 - 値に対応する番号。

以下のコードは D-Link 属性辞書の例です。1 つのファイルとして完結しています。WLAN の要求に合わせて、属性と値を辞書として登録することができます。VENDOR 欄にはベンダ固有の属性値と番号の対応を登録できます。

属性辞書ファイルを作成したら、「etc/raddb」ディレクトリ中に、「dictionary. 会社名」のフォーマットでファイル名を付けて保存してください。（ファイル名の例 : dictionary.D-Link）

```
VENDOR D-Link 6132
#
#D-Link Vendor Specific Extensions
#
#
ATTRIBUTE       D-Link-Wireless-AP-Location           101     string  D-Link
ATTRIBUTE       D-Link-Wireless-AP-Mode               102     integer D-Link
ATTRIBUTE       D-Link-Wireless-AP-Profile-ID         103     integer D-Link
ATTRIBUTE       D-Link-Wireless-AP-Switch-IP          104     ipaddr  D-Link
ATTRIBUTE       D-Link-Wireless-AP-Radio-1-Chan       105     integer D-Link
ATTRIBUTE       D-Link-Wireless-AP-Radio-2-Chan       106     integer D-Link
ATTRIBUTE       D-Link-Wireless-AP-Radio-1-Power      107     integer D-Link
ATTRIBUTE       D-Link-Wireless-AP-Radio-2-Power      108     integer D-Link

VALUE   D-Link-Wireless-AP-Mode               WS-Managed      1
VALUE D-Link-Wireless-AP-Mode                 Standalone      2
VALUE   D-Link-Wireless-AP-Mode               Rogue           3

VALUE D-Link-Wireless-AP-Radio-1-Chan Auto 0
VALUE D-Link-Wireless-AP-Radio-2-Chan Auto 0
VALUE D-Link-Wireless-AP-Radio-1-Power Auto 0
VALUE D-Link-Wireless-AP-Radio-1-Power Minimum 1
VALUE D-Link-Wireless-AP-Radio-1-Power Maximum 100
VALUE D-Link-Wireless-AP-Radio-2-Power Auto 0
VALUE D-Link-Wireless-AP-Radio-2-Power Minimum 1
VALUE D-Link-Wireless-AP-Radio-2-Power Maximum 100
```

属性辞書ファイルを作成したら、FreeRADIUS サーバのメイン辞書ファイルに INCLUDE ステートメントを挿入します。

メイン辞書は「etc/raddb/dictionary」です。以下に dictionary.D-Link という属性辞書ファイルの INCLUDE ステートメントの例を示します。

```
$INCLUDE dictionary.D-Link
```

アクセスポイントの Valid AP データベースへの登録

辞書ファイルに定義した属性は、RADIUS サーバ上の Valid AP データベースにアクセスポイントを設定する際に使用します。設定したファイル名を「etc/raddb/users」とします。以下のコードは、MAC アドレス 00:11:95:a3:32:80 を持つアクセスポイントのデータベースエントリの例です。

注意 FreeRADIUS データベースでは、MAC アドレスに使用する大文字・小文字は区別されます。また各オクテットはハイフン（-）で区切ります。

```
00-11-95-a3-32-80      Auth-Type:=Local,User-Password=="NOPASSWORD"
                       D-Link-Wireless-AP-Mode=WS-Managed,
                       D-Link-Wireless-AP-Location= "Lobby AP",
                       D-Link-Wireless-AP-Profile-ID=1,
                       D-Link-Wireless-AP-Switch-IP=192.168.30.4,
                       D-Link-Wireless-AP-Radio-1-Chan=Auto,
                       D-Link-Wireless-AP-Radio-2-Chan=Auto,
                       D-Link-Wireless-AP-Radio-1-Power=Auto,
                       D-Link-Wireless-AP-Radio-2-Power=Auto
```

B.3 RADIUS サーバでの無線クライアント設定

D-Link アクセスポイントが RADIUS サーバを使用して 802.1X 認証を行い、特定の無線クライアントを使用するユーザの無線ネットワークへのアクセスを許可 / 拒否できるように設定することができます。802.1X 認証を有効にすると、RADIUS サーバ内に登録されたクライアントはユーザベース VLAN や IP トンネリング用のサブネットの割り当てに対応できるようになります。表 B-2 に RADIUS サーバに設定する無線クライアントの属性を示します。

表 B-2　無線クライアントの RADIUS 属性

RADIUS サーバ属性	値の範囲	必須 / 任意
User-Name(1)	1-32 文字の半角英数字	必須
User-Password(2)	1-128 文字の半角英数字	必須
Tunnel-Medium-Type(65)	802	任意

クライアントの MAC 認証のための RADIUS 設定

D-Link アクセスポイントが RADIUS ベースの MAC 認証して、特定の無線クライアントを使用するユーザの無線ネットワークへのアクセスを許可 / 拒否できるように設定することができます。この方法は 802.1X よりも安全性は低くなりますが、802.1X をサポートしない無線クライアントにも適用できるという利点があります。

登録したアドレスは、AP プロファイル内のグローバルデフォルトの動作に基づいて、アクセス許可または拒否されます。

表 B-3 に RADIUS サーバに設定する属性を示します。

表 B-3　無線クライアント MAC 認証用の RADIUS 属性

項目	説明	値の範囲	必須 / 任意
User-Name(1)	クライアントの MAC アドレス	有効 MAC アドレス	必須
User-Password(2)	クライアントの MAC エントリ検索用の固定パスワード	NOPASSWORD	必須

B.4 FreeRADIUS を使用した無線クライアント設定例

FreeRADIUS などの外部 RADIUS サーバが起動中のサーバを使用して、アクセスポイントに接続を試みるユーザを認証することができます。認証はアクセスに使用する無線クライアントではなく、ユーザ名とパスワードを元に行います。ユーザがサーバにより認証された後でも、RADIUS サーバはそのユーザに対して VLAN を割り当てることができます。

ユーザベースの認証に加え、無線クライアントの MAC アドレスベースの認証して、アクセスポイントへのアクセスを許可 / 拒否することができます。

ユーザベース認証とダイナミック VLAN の設定

外部 RADIUS サーバ内にユーザエントリを登録することにより、ユーザ証明書をアクセスポイント宛てに送信させて、動的にユーザを VLAN に割り当てることができます。

ダイナミック VLAN では、ユーザを VLAN に割り当てるとスイッチがこの情報を使用してスイッチ上のポートの設定を自動的に行います。VLAN の選択は、通常「どのユーザと接続するのか」によって決定されます。RADIUS サーバはアクセスポイントに対し、ユーザ認証情報の一部として「選択された VLAN」を伝えます。これにより、ダイナミック VLAN を利用するユーザは、干渉を受けることなく、またスイッチ上で設定変更することなく場所を移動することができます。
B.1 外部 RADIUS サーバが VLAN を管理するためには、アクセスポイントに選択した VLAN の情報を伝えるために、サーバに Access-Accept メッセージ中にトンネル属性を含むように設定します。本属性については RFC 2868 に、またダイナミック VLAN 中での属性の使用法については RFC 3580 に規定されています。
RFC 3580 で規定されている VLAN 属性は以下の通りです。

- Tunnel-Type=VLAN(13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

注意 FreeRADIUS 辞書では文字列の 802 を整数の 6 とマッピングしています。このためクライアントエントリでは、Tunnel-Medium-Type に 6 を使用しています。

FreeRADIUS を使用して、ユーザを作成して特定の VLAN に割り当てるには、ユーザアカウント情報を持つ「etc/raddb/users」ファイルを開き、新規ユーザとして追加します。

以下にユーザファイル中のユーザエントリの例を示します。ユーザ名が「johndoe」、パスワードが「test1234」のユーザは「VLAN 77」に割り当てられています。

```
johndoe Auth-Type:=EAP,User-Password== "test1234"
        Tunnel-Type="VLAN",
        Tunnel-Medium-Type="IEEE-802",
        Tunnel-Private-Group-ID="77",
```

すべてのクライアントに対し、「Tunnel-Type」と「Tunnel-Medium-Type」には同じ値を設定します。「Tunnel-Private-Group-ID」は選択されたVLAN ID であり、ユーザにより異なります。

注意 「Tunnel-Private-Group-ID」にはアクセスポイントの管理 VLAN ID を使用しないでください。

動的に割り当てられる RADIUS VLAN はアクセスポイントの管理 VLAN と異なる必要があります。RADIUS サーバがクライアントに対して、管理VLAN として使用している VLAN をダイナミック VLAN に割り当てようとすると、アクセスポイントはダイナミック VLAN の割り当てを無視し、新しく接続するクライアントにはその VAP のデフォルト VLAN を割り当てます。再認証するクライアントは、以前の VLAN ID を保持します。

すべてのアクセスポイントにおいて、管理 VLAN ID はデフォルトで 1 に設定されています。これを変更するためには、CLI から **`set management vlan-id`** コマンドを実行します。

「etc/raddb/users」の変更後、RADIUS サーバデーモンを再起動して変更内容を適用する必要があります。

MAC 認証の設定

各ネットワークについて、クライアントの MAC 認証にローカルデータベースを使用するか、または RADIUS データベースを使用するかを指定します。RADIUS ベースのクライアントを MAC 認証するためには、「etc/raddb/users」ファイルに各クライアントの MAC アドレスを登録します。スイッチ上で MAC 認証のデフォルト動作が「Allow（許可）」と設定されている場合、ファイル中に登録されたクライアントのみがアクセスポイントを経由してネットワークにアクセスすることを許可されます。逆にデフォルトアクションが「Deny（拒否）」の場合、ファイル中に登録のあるクライアントはアクセスポイントに認証されなくなります。

以下に「etc/raddb/users」ファイル内のクライアントのエントリ例を示します。

```
00-0F-FE-1C-F2-67 Auth-Type:=Local,User-Password== "NOPASSWORD"
```

注意 パスワードは、常に「NOPASSWORD」とし、MAC アドレスはコロンではなく、ハイフンで区切ります。

付録 C　L3 ローミング設定例

VLAN ローミングは VLAN トランキング（VLAN に SSID を関連させる）または L3 トンネル（トンネルサブネットに SSID を関連させる）を使用することで実行することができます。ここでは、L3 ローミング機能を必要とするネットワークにおいての D-Link 統合スイッチの設定例を紹介します。WLAN 上での L3 トンネリングの実施に必要となる以下の機能の設定方法を含め説明します。

- WLAN とトンネルインタフェースの設定
- L3 トンネルネットワークの設定
- DHCP リレーと DHCP サーバの設定

C.1 WLAN とトンネルインタフェースの設定

以下の図に無線ローミングをサポートするために L3 トンネリングを使用するネットワークの例を示します。すべてのクライアントが L3 ローミングに使用するサブネットは 192.168.60.0/24 です。設定例はすべて図中のネットワーク情報を元にしています。

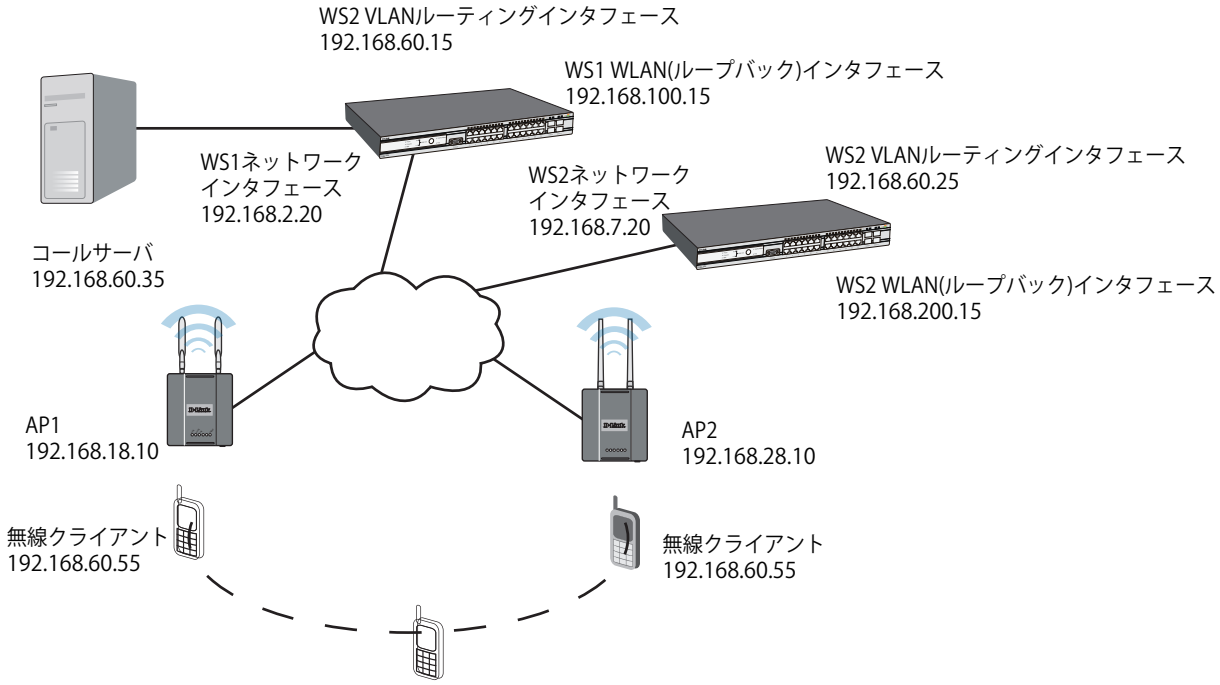


図 C-1　L3 トンネル用サブネットを持つネットワーク例

例として使用するネットワークは以下のような前提条件を持つものとします。

- 各スイッチ、コールサーバ、およびローミングする無線クライアントの VLAN ルーティングインタフェースはすべて L3 トンネルサブネット上に存在します。
- 各ピアスイッチは同一の L3 トンネルサブネット上に論理インタフェースを持ち、クライアントがネットワーク上のすべてのピアスイッチの管理下にあるアクセスポイント間をローミングできるようにします。
- ピアスイッチ同士は同一の物理サブネット上に存在しません。
- アクセスポイントは、スイッチと同一のサブネットや L3 トンネルサブネット上に存在しません。
- コールサーバは 1 台の統合スイッチに物理接続され、コールサーバが使用するポートにはトンネルされるサブネットの VLAN ルーティングインタフェースに設定される VLAN ID が割り当てられます。
- 各スイッチは WLAN 機能用にループバックインタフェースを使用し、ループバックインタフェースは L3 トンネルサブネットとは異なるネットワーク上に存在します。
- 各スイッチ上でルーティング機能が有効になっています。
- ネットワークデバイスはループバックサブネットと L3 トンネルサブネットへの経路を持ちます。ホストは各スイッチ上のループバックインタフェースと L3 トンネルインタフェースに ping できます。
- 各スイッチにおいて DHCP リレーが有効になっており、ネットワーク上の DHCP サーバが無線クライアントに対し IP アドレスを割り付けることができます。
- 無線クライアントは L3 トンネルサブネット中の IP アドレスを取得し、ローミングを通じ、その IP アドレスを保持します。

注意　アクセスポイント、ピアスイッチ、および他のルータはトンネルされるルーティングインタフェースに接続することはできません。

電話のシステムによっては、コールサーバを電話機と同じサブネット上に配置する必要がある場合があります。D-Link トンネリング機能はそのような構成をサポートできます。

L3 ローミング機能を持つネットワークの計画時には、以下の注意すべき項目があります。

- L3 トンネリングを利用するパケットには、カプセル化に使用する 20 バイトの IP ヘッダが付加されます。
- 大きいフレームに対応するために、すべての中継ポートと WLAN スイッチポート上で MTU サイズを拡大することができます。
- トンネリングを IP テレフォニー用のみに使用する場合、またはトンネリングを使用するすべての無線クライアント上で MTU サイズを 1480 に設定している場合は、ネットワーク内での MTU サイズを拡大する必要はありません。
- L3 トンネル内のトラフィックについては、スイッチは IPv4 ユニキャストフレームをハードウェア転送します。また、マルチキャストや非 IP のトラフィックについてはソフトウェア転送します。
- L3 トンネリングネットワーク上のマルチキャストや非 IP トラフィックによりネットワーク輻輳が発生することがあります。
- L3 トンネルインタフェース上で IPv6 またはマルチキャストトラフィックが有効である場合、無線トンネリングは動作しません。
- 無線サブネットはスイッチにとってローカルであるため、L3 トンネルネットワークを使用するすべてのデバイスのアドレス情報は ARP キャッシュに保存されます。そのため、ARP キャッシュは予想よりも早く一杯になる可能性があります。
- トンネルクライアントがピアスイッチと共に使用される場合、ピアスイッチの一方は、トンネルクライアントのデフォルトゲートウェイとして設定される必要があります。通常、デフォルトゲートウェイはクライアントのサブネットから他のサブネットにすべてのトラフィックを送信しますが、ピアスイッチネットワークでは、クライアントが関連する AP を管理する統合スイッチは、リモートサブネットにフレームを送信します。つまり、各ピアスイッチはネットワーク内のあらゆるサブネットにフレームを送信することをルーティングテーブルエントリを持つ必要があるということを意味します。

無線機能でループバックインタフェースの使用

ループバックインタフェースを定義することにより、複数のルーティングインタフェースが存在する場合に、無線機能の IP アドレスとしてどのルーティングインタフェースを使用するかを指定することができます。ループバックインタフェースを使用すれば、無線機能用の IP アドレスとして常に同じものを使用できます。

注意 上記のループバックインタフェースとは、自分自身を示す IP アドレス 127.0.0.1 を持つループバックインタフェースとは異なります。スイッチの無線インタフェースとしてループバックインタフェースを設定する場合は、それが永続的に論理的なインタフェースであり、IP アドレス 127.0.0.1 ではないということが重要になります。ループバックインタフェースには専用のサブネットを設け、ネットワーク中の他のデバイスはループバックインタフェースにアクセス可能である必要があります。

他のデバイスがループバックインタフェースを見つけることができるように、スタティックルートを定義する必要があります。

ループバックインタフェースを定義すると、ループバックインタフェースはダウンしなくなるという利点があります。反対に、ネットワーク構成が複雑になるという欠点があります。これはループバックインタフェースは自身のサブネットに属し、ネットワークの他のデバイスはそのサブネットまでの到達方法を知っている必要があるためです。

ネットワーク中の統合スイッチと管理対象のアクセスポイント間には、ルートが存在する必要があります。アクセスポイントから統合スイッチの無線インタフェースに指定されたループバックインタフェースの IP アドレスへの ping 送信が可能である必要があります。

以下の手順では、CLI を使用して、ルーティング機能を有効にし、ルーティングインタフェースまたはループバックインタフェースの IP アドレスを設定する例を示します。

1. CLI にログインし、Global Config モードに遷移します。

```
(System-Prompt)
User:admin
Password:
(System-Prompt) >enable
Password:
(System-Prompt) #config
(System-Prompt) (Config)#
```

2. ルーティング機能を有効にします。

```
(System-Prompt) (Config)#ip routing
```

3. ループバックインタフェース 0 の Interface Config mode に移行し、IP アドレスとサブネットマスクを登録します。

```
(System-Prompt) (Config)#interface loopback 0
(System-Prompt) (Interface loopback 0)#ip address 192.168.100.15 255.255.255.255
```

CLI の他にも、Web インタフェースや SNMP を使用して、ルーティング情報を有効にしたり、IP アドレスを設定することができます。以下に、Web インタフェースを使用して、スイッチ上でルーティング情報を有効にし、IP アドレスを設定する方法を示します。

1. Web インタフェースにログインし、**LAN タブ > L3 Features > IP > Configuration** とクリックして、「IP Configuration」ページを表示します。

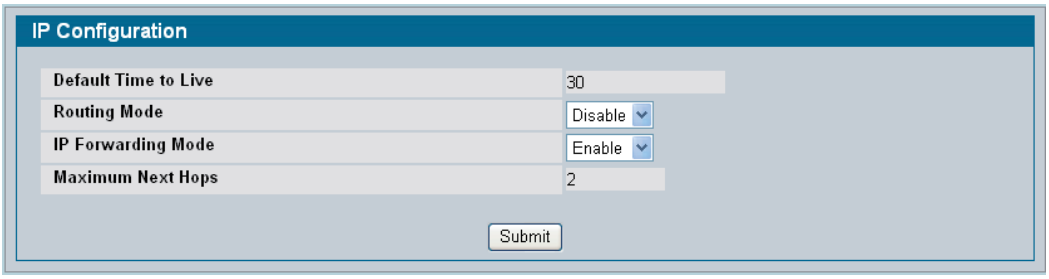


図 C-2　IP Configuration 画面

2. 「Routing Mode」プルダウンメニューから「Enable」を選択し「Submit」ボタンをクリックします。

3. ループバックインタフェースを作成するためには、**LAN タブ > L3 Features > Loopbacks > Configuration** とクリックします。

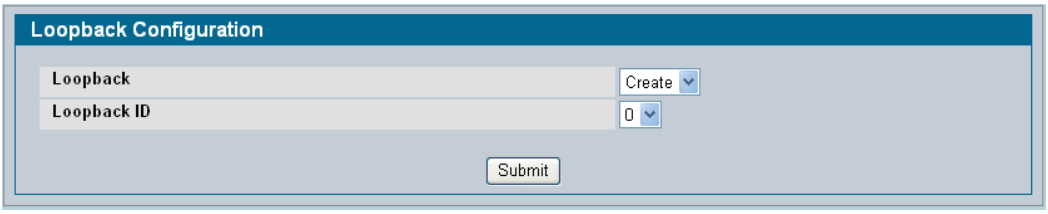


図 C-3　IP Configuration 画面

4. 「Loopback」プルダウンメニューから「Create」を選択し「Submit」ボタンをクリックします。

5. IPv4 アドレスとサブネットマスクをそれぞれの欄に入力し、「Submit」ボタンをクリックします。

VLAN ルーティングインタフェースの登録

D-Link 統合スイッチと D-Link アクセスポイントは、物理ネットワークを論理的に分離させるために VLAN（仮想 LAN）をサポートしています。VLAN 機能を使用すると、無線ネットワークを VAP ベースに分割することができます。VLAN ルーティングインタフェースにより、異なるサブネット間をまたいだ VLAN が実現され、L3 トンネリングに利用することができます。

図 C-1 中の WS1 と WS2 は L3 トンネルサブネット上に VLAN ルーティングインタフェースを持ちます。以下のコマンドは、WS1 に VLAN ID 200 と VLAN ルーティングインタフェースの IP アドレス 292.168.60.15 を設定する方法を示します。

1. VLAN config モードに入り、VLAN を登録して VLAN 名を与えます。

```
(switch-prompt) #vlan database
(switch-prompt) (Vlan)#vlan 200
(switch-prompt) (Vlan)#vlan name 200"L3 Tunnel"
```

2. VLAN 200 に VLAN ルーティングインタフェースを設定します。

```
(switch-prompt) (Vlan)#vlan routing 200
```

3. Privileged EXEC モードに遷移し、VLAN ルーティングインタフェースの設定を確認します。

```
(switch-prompt) (Vlan)#exit
(switch-prompt) #show ip vlan

MAC Address used by Routing VLANs:00:00:00:01:00:02

                Logical
    VLAN ID     Interface          IP Address        Subnet Mask
    ------    ---------------   -----------------   ------------------------
    200       0/4/1             0.0.0.0             0.0.0.0
```

新しく設定した VLAN ルーティングインタフェースは、0/4/1（ユニット / スロット / ポート）です。スタッキング以外の構成では、4/1 の場合があります。

4. 設定した VLAN ルーティングインタフェースの interface configuration モードに入ります。

```
(switch-prompt) #configure
(switch-prompt) (Config)#interface 0/4/1
```

5. IP アドレスを指定してルーティングを有効にします。

```
(switch-prompt) (Interface 0/4/1)#ip address 192.168.60.15 255.255.255.0
(switch-prompt) (Interface 0/4/1)#routing
```

6. VLAN 200 にコールサーバに接続するポートを追加します。（この例ではコールサーバはポート 3 に接続されます。）

```
(switch-prompt) (Config)#interface 1/0/3
(switch-prompt) (Interface 1/0/3)#vlan participation include 200
```

Web インタフェースを使用して同じ設定を行う場合は、以下の手順を実行してください。

1. **LAN タブ > L2 Features > VLAN > VLAN Configuration** をクリックし、以下の画面を表示します。VLAN を作成して名前を登録します。また VLAN 200 にコールサーバに接続するポートを追加します。（この例ではコールサーバはポート 3 に接続されます。）

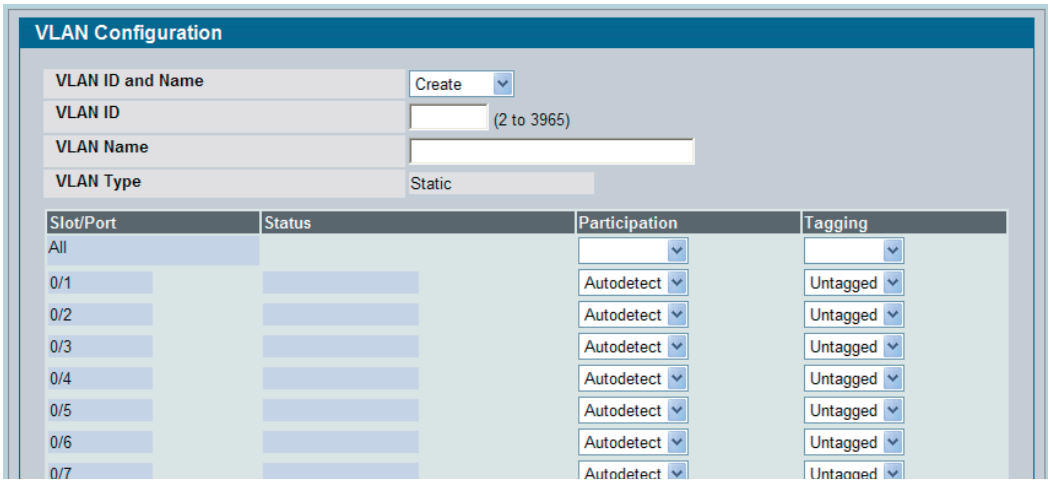


図 C-4　VLAN の作成とポートの追加

2. **LAN タブ > L3 Features > VLAN Routing Configuration** ページを開き、VLAN 200 に VLAN ルーティングインタフェースを設定します。

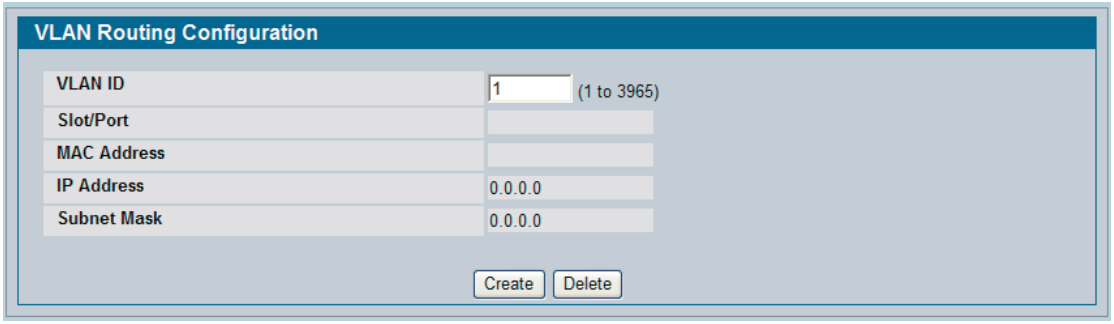


図 C-5　VLAN ルーティングインタフェースの設定

3. **LAN タブ > L3 Features > IP > Interface Configuration** ページを開き、インタフェースに IP アドレスとサブネットマスクを設定し、ルーティングを有効にします。

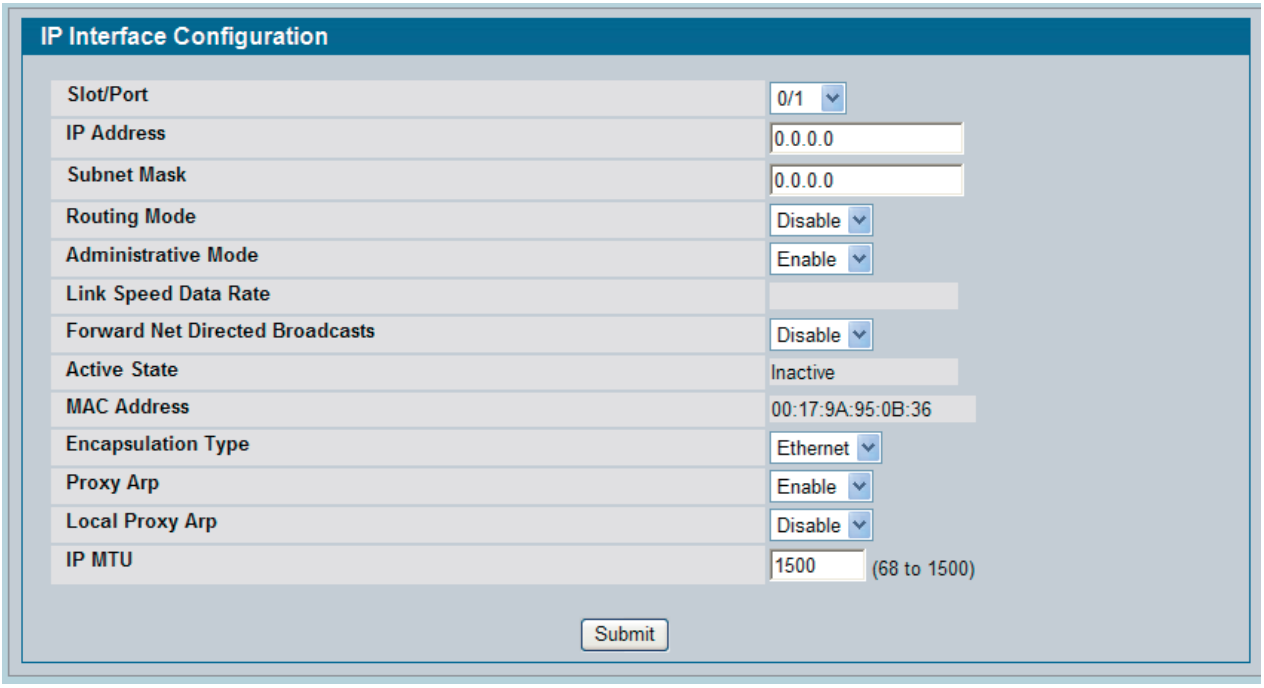


図 C-6　IP アドレスとサブネットマスクの設定

4. **LAN タブ > Monitoring > L3 Status > VLAN Routing Summary** ページを開き、VLAN ルーティングインタフェースのサマリ情報を確認します。

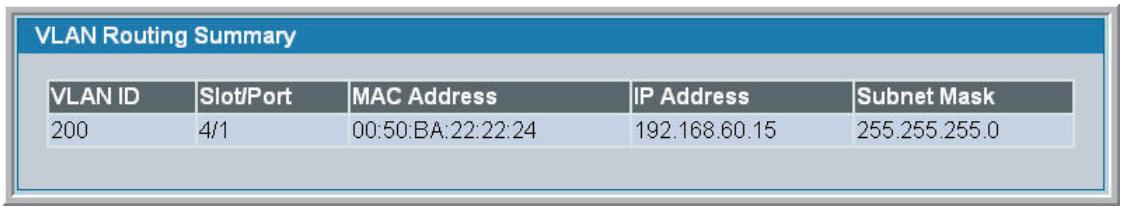


図 C-7　VLAN ルーティングインタフェース情報の確認

C.2 L3 トンネルネットワークの設定

L3 トンネリングの設定を終えたら、無線クライアントがローミングに使用する可能性のあるアクセスポイントに適用した AP プロファイル中の VAP に、ネットワークが設定されていることを確認します。AP プロファイルを変更した場合は、アクセスポイントに再度適用してアクセスポイントを再起動します。

注意 L3 ローミングが有効である場合、ネットワークの VLAN ID は使用されません。スイッチはトンネルを使用するパケットに管理 VLAN ID（設定がある場合）を挿入します。

次の例では、L3 トンネルネットワークはデフォルト AP プロファイル内の Network 3 上に設定されます。ネットワークの SSID は "L3 Tunnel" で、セキュリティ方式には "WPA Enterprise" を使用します。

CLI を使用した L3 ローミング設定例

次に CLI を使用して D-Link 統合スイッチに L3 ローミングを設定する例を示します。Web インタフェースによる設定手順については、この後に記載しています。

1. Network 3 の network configuration モードに入ります。

```
(switch-prompt) #configure
(switch-prompt) (Config)#wireless
(switch-prompt) (Config-wireless)#network 3
```

2. ネットワーク名（SSID）を登録します。

```
(switch-prompt) (Config-network)#ssid "L3 Tunnel"
```

3. 無線クライアントからのアクセスを制御するセキュリティを指定します。本ネットワークでは WPA Enterprise を指定します。管理者は L3 トンネルネットワークへのアクセスを許可するクライアントに対しても、セキュリティ設定をする必要があります。

```
(switch-prompt) (Config-network)#security mode wpa-enterprise
```

4. L3 ローミングを有効にします。

```
(switch-prompt) (Config-network)#tunnel
```

5. トンネル用の L3 ネットワーク IP アドレスとサブネットマスクを設定します。

注意 ここで指定するネットワーク IP アドレスは、VLAN ルーティングインタフェース（148 ページの「VLAN ルーティングインタフェースの登録」で作成）が使用するものと同じサブネットである必要があります。

```
(switch-prompt) (Config-network)#tunnel subnet 192.168.60.0 mask 255.255.255.0
```

6. Network モードを終了し、デフォルトプロファイル（Profile 1）の AP profile configuration モードに入ります。

```
(switch-prompt) (Config-network)#exit
(switch-prompt) (Config-wireless)#ap profile 1
```

7. 設定する無線インタフェースの AP Profile Radio Config モードに入ります。
この例では、L3 トンネルネットワークは Radio 1（初期値で 802.11g 指定）を使用します。

```
(switch-prompt) (Config-ap-profile)#radio 1
```

8. VAP 2 の AP Profile VAP Config モードに入り、VAP を有効にします。
デフォルトネットワークの VAP 0 のみが、デフォルトで有効に設定されています。この例では、ゲストネットワークが VAP 0、社内ネットワークが VAP 1、L3 トンネルネットワークが VAP 2 を使用するとします。

```
(switch-prompt) (Config-ap-radio)#vap 2
(switch-prompt) (Config-ap-profile-vap)#enable
```

9. L3 トンネルネットワーク（ネットワーク 3）を VAP 2 に割り当てます。

```
(switch-prompt) (Config-ap-profile-vap)#network 3
```

10. 「Ctrl」キーと「Z」キーを同時に押下して Privileged EXEC モードに戻り、ネットワーク設定を確認します。「L3 Tunnel Status」が「Configured」となっているか、また他のネットワーク設定が正しく登録されているかをチェックします。

```
(switch-prompt) #show wireless network 3

Network ID..................................... 3
SSID........................................... L3 Tunnel
Default VLAN................................... 1
Hide SSID...................................... Disable
Deny Broadcast................................. Disable
L3 Tunnel Mode................................. Enable
L3 Tunnel Status............................... Configured
L3 Tunnel Subnet IP............................ 192.168.60.0
L3 Tunnel Subnet Mask.......................... 255.255.255.0
Security Mode.................................. WPA Enterprise
MAC Authentication............................. Disable
RADIUS Use AP Profile.......................... Enable
RADIUS Server IP............................... 0.0.0.0
RADIUS Secret Configured....................... No
RADIUS Accounting.............................. Disable
WPA Versions................................... WPA/WPA2
WPA Ciphers.................................... TKIP
WPA Key Type................................... ASCII
WPA Key.....................................
WPA2 Pre-Authentication.......................  Enable
WPA2 Pre-Authentication Limit(minutes)......... 0
WPA2 Pre-Authentication Timeout(minutes)....... 0
--More--or(q)uit
WPA2 Key Forwarding............................ Enable
WPA2 Key Caching Holdtime(minutes)............. 10
WEP Authentication Type........................ Open System
WEP Key Type................................... HEX
WEP Key Length(bits)........................... 128
WEP Transfer Key Index......................... 1
WEP Key 1.....................................
WEP Key 2.....................................
WEP Key 3.....................................
WEP Key 4.....................................
```

「L3 Tunnel Status」に表示される値は、トンネリング機能の設定状態を確認するために重要です。以下の表に、表示される値とその値が示す意味を示します。

表 C-1　L3 トンネリング設定状態

L3 Tunnel Status の値	説明
None	以下のいずれかの原因により、状態が表示できません。 • WLAN の動作状態が無効になっている。 • L3 トンネル機能が無効に設定されている。 • ネットワークに AP プロファイルが関連付けされていない。ネットワークを作成・編集し、L3 トンネリングを定義したが、AP プロファイルにそのネットワークを使用する VAP の登録がない。
Configured	L3 トンネルの登録が完了し、本プロファイルを使用するアクセスポイントに適用可能な状態にあります。
Not Configured-Routing Disabled	ルーティングインタフェース上でルーティングが無効に設定されています。
Not Configured-No Routing Interface	以下のいずれかの原因により、本メッセージが表示されています。 • L3 トンネルネットワーク用のルーティングインタフェースが存在しない。 • ルーティングインタフェース上で IPv6 が有効になっている。 • ルーティングインタフェース上で IP マルチキャストが有効になっている。 • トンネル用サブネットアドレスがルーティングインタフェースと適合しない。 この例では、VLAN ルーティングインタフェースは 192.168.60.15/24 の IP アドレスを持ち、L3 トンネルサブネットは 192.168.60.0/24 と指定されています。このような場合には、トンネルサブネットはルーティングインタフェースに適合していると言えます。

11. Privileged EXEC モードで、デフォルトプロファイル（Profile 1）を使用するアクセスポイントに対して、変更後のデフォルトプロファイルを適用します。

```
(switch-prompt)#wireless ap profile apply 1
```

アクセスポイントの更新が完了すると、L3 トンネルネットワークはデフォルトプロファイルを使用するすべてのアクセスポイント上で利用可能となります。L3 トンネル SSID を使用してアクセスポイントに接続するユーザは、通信が途切れることなく、それらすべてのアクセスポイント間でローミングすることができます。

各アクセスポイントから、スイッチのループバック IP アドレスや L3 トンネルに使用するルーティングインタフェースの IP アドレスに ping を送信し、接続性を確認してください。Privileged EXEC モードから、**wireless ap debug** <macaddr> コマンドを実行してアクセスポイントでのデバッグ機能を有効にすると、アクセスポイントに Telnet 接続することができます。

無線クライアントがトンネルサブネットにより接続可能になれば、ping コマンドを使用し、MTU サイズを変更して、希望するパケットサイズがトンネル内を通過できるようにします。

Windows クライアントの場合は、「-l<size>」によりパケットサイズを指定し、「-f」によりパケットのフラグメント化を禁止します。以下に例を示します。

```
ping-l 1542-f 192.168.60.15
```

Unix の場合は、"-s<size>" によりパケットサイズを指定し、"-M do" によりパケットのフラグメント化を禁止します。以下に例を示します。

```
ping-s 1542-M do 192.168.60.15
```

Web インタフェースを使用した L3 ローミングの設定例

スイッチ上で Web インタフェースを使用して、L3 トンネルネットワークを設定する手順を以下に示します。

1. **WLAN タブ > Administration > Basic Setup** の順にメニューをクリックし、「SSID」タブを選択して設定する SSID の左側にあるチェックボックスを選択して「Edit」ボタンをクリックします。

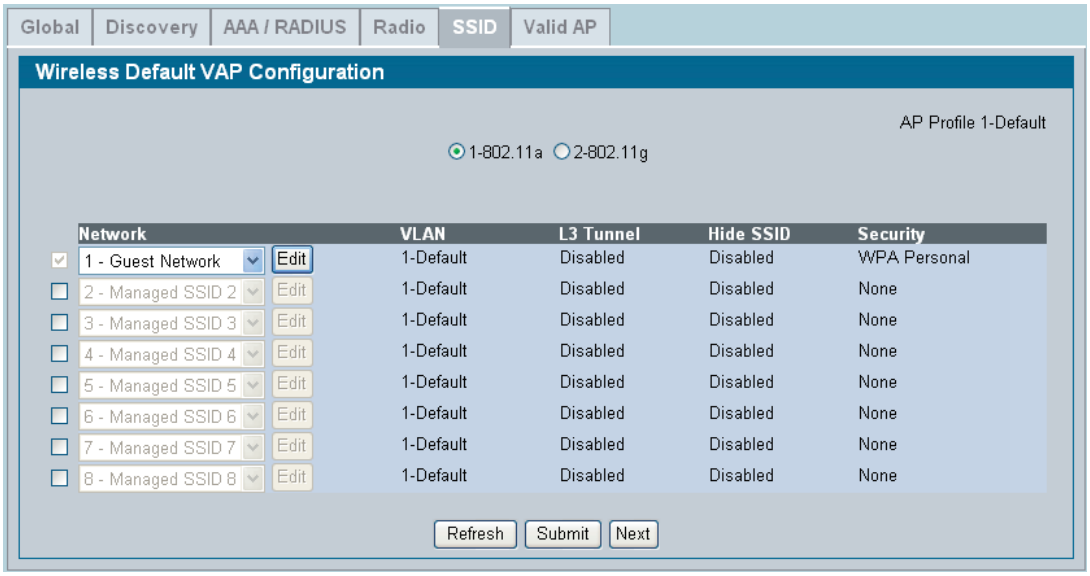


図 C-8　SSID の設定

2. 「Wireless Network Configuration」ページで、以下の値を設定します。

- SSID - L3 Tunnel
- L3 Tunnel チェックボックス - 選択
- L3 Tunnel Subnet - 192.168.60.0
- L3 Tunnel Mask - 255.255.255.0
- Security - WPA/PSK

「L3 Tunnel Subnet」には 148 ページの「VLAN ルーティングインタフェースの登録」で作成した VLAN ルーティングインタフェースの IP アドレスを入力します。

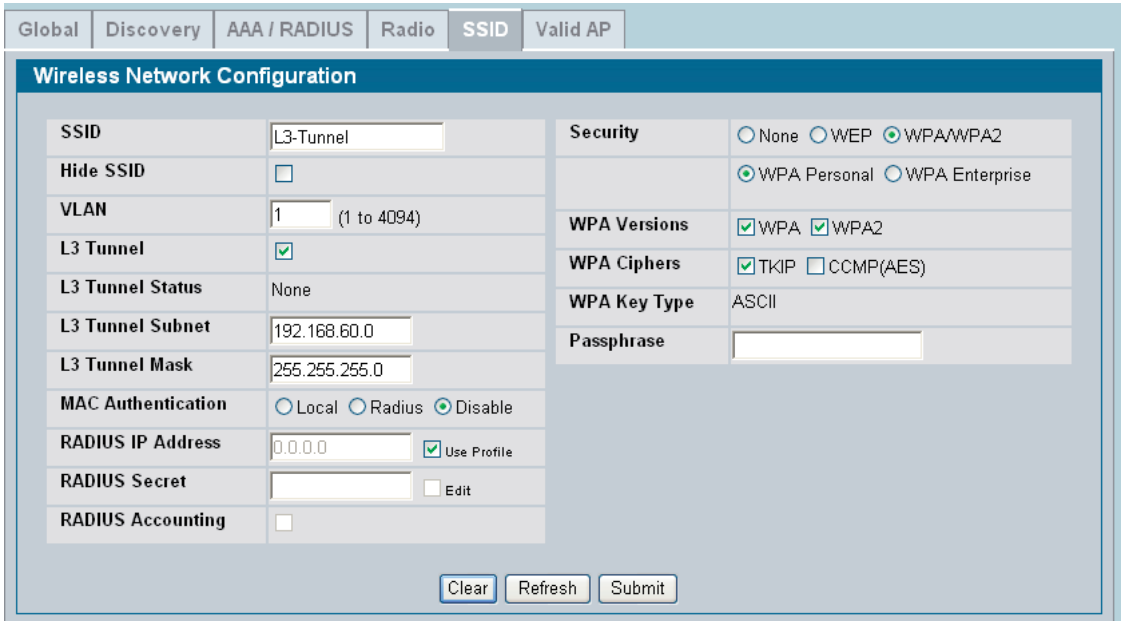


図 C-9　VLAN ルーティングインタフェース IP アドレスの入力

3. 「Submit」ボタンをクリックして、L3 トンネルネットワークコンフィグレーションに設定を保存します。

4. 「L3 Tunnel Status」欄にて L3 トンネルの設定状態を確認します。

5. **WLAN タブ > Administration > Advanced Configuration > AP Profiles** ページにて、アクセスポイントにプロファイルの変更を適用します。

6. デフォルトプロファイルのチェックボックスを選択して「Apply」ボタンをクリックします。

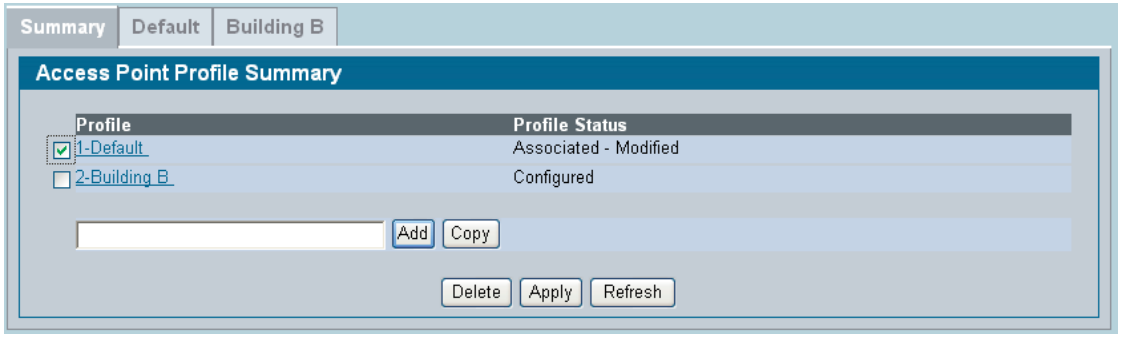


図 C-10　プロファイルの変更の適用

プロファイルが更新されると、統合スイッチはデフォルトプロファイルを使用するアクセスポイントに L3 トンネルネットワークを追加します。

C.3 DHCP リレーと DHCP サーバの設定

統合スイッチを DHCP サーバとして使用している、またはすべてのデバイスにスタティック IP アドレスを設定している場合を除き、スイッチ上で DHCP リレー機能を有効にすることにより、ローミング中の無線クライアントからの DHCP 要求をネットワーク上の DHCP サーバに転送する必要があります。

統合スイッチを DHCP サーバとして使用する場合には、DHCP サーバの設定と無線クライアントのアドレスプール設定を行う必要があります。

リレーエージェントの設定

Global Config モードにおいて以下のコマンドを実行し、スイッチ上で BOOTP および DHCP リレー機能を有効にします。

```
(switch-prompt)(Config)#bootpdhcprelay enable
```

Global Config モードにおいて以下のコマンドを実行し、無線クライアントに IP アドレスを割り当てる BOOTP または DHCP サーバのアドレスを指定します。

```
(switch-prompt)(Config)#bootpdhcprelay serverip 192.168.30.2
```

Web インタフェースを使用してスイッチ上に BOOTP と DHCP リレーを設定するためには、**LAN タブ > L3 Features > BOOTP/DHCP Relay Agent Configuration** の順にメニューをクリックし、以下の画面を表示します。サーバの IP アドレスを入力し、「Admin Mode」を「Enable」（有効）にし、「Submit」ボタンをクリックします。

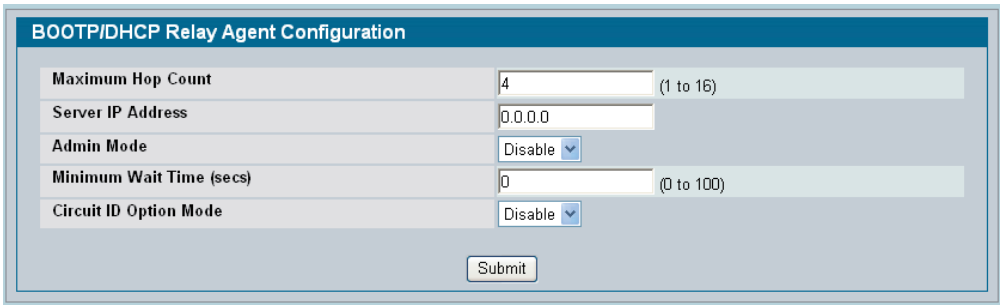


図 C-11　DHCP リレーの設定

DHCP サーバの設定

スイッチ上に DHCP サーバを設定するためには、グローバル DHCP 設定とクライアントのアドレスプールの設定します。以下に L3 トンネルネットワークでの無線クライアントのアドレスプール作成例を示します。アドレスプールを追加して、統合スイッチ上の DHCP サーバが他のネットワーク（ゲストネットワークや社内 LAN など）を使用するクライアントに IP アドレスを割り当てることもできます。
以下に L3 トンネルネットワークに接続するクライアント用に使用する DHCP サーバのコマンド設定方法を示します。

1. Global Config モードで DHCP 機能を有効にします。

```
(switch-prompt) (Config)#service dhcp
```

2. 192.168.60.1 から 192.168.60.50 までの IP アドレス（WS1、WS2 およびコールサーバのアドレスを含む）を割り当て可能なアドレスから除外します。

```
(switch-prompt) (Config)#ip dhcp excluded-address 192.168.60.1 192.168.60.50
```

3. アドレスプールを作成します。

```
(switch-prompt) (Config)#ip dhcp pool vlan200
```

4. L3 トンネルサブネットとサブネットマスクを VLAN 200 を使用するクライアントのネットワークアドレスとして設定します。

```
(switch-prompt) (Config)#network 192.168.60.0 255.255.255.0
```

5. アドレスプールにデフォルトルータを登録します。

```
(switch-prompt) (Config)#default-router 192.168.60.1
```

前頁と同じ設定を Web インタフェースで行うには、以下の手順を実行してください。

1. **LAN タブ > Administration > DHCP Server > Global Configuration** の順にメニューをクリックし、以下の画面を表示します。「Admin Mode」を「Enable」（有効）にし、無線クライアントへの割り当てをしない IP アドレス範囲を指定し、「Submit」ボタンをクリックします。

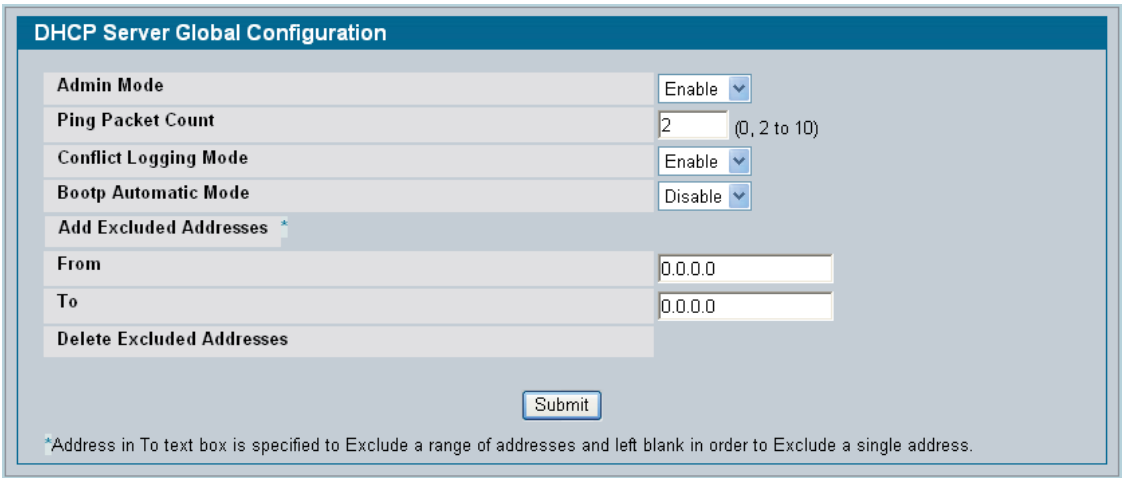


図 C-12　割り当てを行わない IP アドレス範囲の指定

2. **LAN タブ > Administration > DHCP Server > Pool Configuration** の順にメニューをクリックし、以下の画面を表示します。

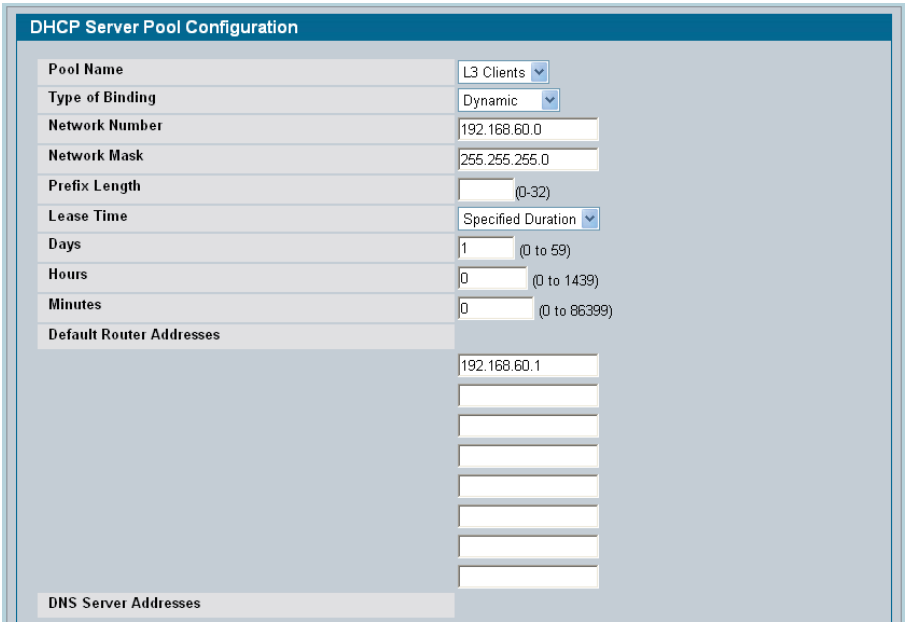


図 C-13　DHCP サーバ設定の適用

3. 「Pool Name」欄に、アドレスプールの名前を入力し、「Type of Binding」プルダウンメニューから「Dynamic」を選択します。

4. 「Network Number」、「Network Mask」、「Default Router Addresses」のそれぞれの欄に入力し「Submit」ボタンをクリックします。

付録 D　QoS 制御について

D-Link 統合アクセスシステムにおける QoS（Quality of Service）機能は、複数のキューにパラメータを指定することで、従来の IP データをはじめ VoIP（Voice over IP）や音声、映像、ストリーミングメディアなどの多くの無線トラフィックに対してスループットとパフォーマンスの向上を可能にします。

サービスの品質に最も影響を与える要素は、電波にアクセスしようとするクライアント数の増加や、繁忙期に増加したトラフィックが帯域の獲得を巡り争うことによるネットワークの輻輳です。混んでいるネットワークにおいて、最もサービス品質の低下が顕著になるのは、ビデオ、VoIP やストリーミングメディアなどの時間に依存するタイプのアプリケーションです。

サービス品質のばらつきに影響を受けることの少ない通常のデータファイルとは異なり、ビデオ、VoIP やストリーミングメディアは、そのパケット送信を、決まった順番で一定の速度で、またできるだけ遅延が発生しないように行わなければなりません。サービス品質が損なわれれば音声や映像にひずみが生じることになります。

QoS とロードバランシング

ロードバランシングと QoS 技術を組み合わせることで、ネットワークの混雑時でも、時間依存型のアプリケーションに高いサービス品質を提供することができます。ロードバランシングでは、クライアントの接続とアクセスポイントの使用率にしきい値を設けます。QoS とは、1 台のアクセスポイントにおいて種類の異なる無線トラフィックに優先順位を設け、それに基づいて帯域とネットワークアクセスを割り当てするための手段です。

802.11e と WMM 標準のサポート

QoS には、共用ネットワーク上でデータストリームを制御するためのさまざまな技術が盛り込まれています。IEEE 802.11e タスクグループは、無線ネットワークにおいての伝送品質およびサービスの安定供給を規定する QoS 標準を策定中です。QoS はジッタの量や待ち時間、パケット損失率を制限しながらネットワークの輻輳を最小限に抑え、良質なネットワークサービスを提供すべく設計されています。また、時間依存型やミッションクリティカルな基幹アプリケーション専用の帯域をサポートし、それらのトラフィックに優先権を与えるチャンネルアクセスを実現します。

同タスクグループの目標は、他のすべての 802.11 ワーキンググループと同様に、各種ベンダのコンポーネントでインターオペラビリティを可能とする、QoS 機能実現のための標準的手法を供給することです。

D-Link アクセスポイントは 802.11e ドラフトのサブセットとして開発される WMM（Wi-Fi Multimedia）標準に基づいた QoS を提供します。

アクセスポイントと無線クライアント（ノート PC、家庭用電化製品等）共に、Wi-Fi 認定の WMM に対応しています。

トラフィックフローの調整

D-Link 統合アクセスシステムでの QoS 設定は、各種無線トラフィック用のキューにパラメータを設定することにより行います。送信するメディアが必要とする条件に基づき、各キューに対して異なるパケット送信時の最小・最大待ち時間を指定することができます。音声、映像、マルチメディアや基幹アプリケーションに対しては、自動的に伝送遅延が最小になるように調整され、一般的な IP データにはベストエフォート型のサービスが割り振られます。

例えば、時間に依存する音声、映像、マルチメディアにはその伝送に高い優先権（チャンネルアクセスへの待ち時間の低減）が与えられ、反対に、比較的時間に依存はしないがデータ量が多い他のアプリケーションや IP データの待ち時間は、長めに設定されます。

D-Link 統合アクセスシステムは、IEEE、WMM 標準に基づく QoS を実装しています。パケットのタグ付けおよび複数のキューの作成に Linux ベースのキュークラスが使用されます。それらのキューにより、優先順位の決定と送信データの種類に基づいたルーティングが提供されます。

キューに使用するパラメータは管理者用ユーザインタフェースを使用して設定できます。

QoS キューとパケット内の DSCP

D-Link 統合アクセスシステムでは IP ヘッダ中の WMM 情報を DSCP（Diff-Serv Code Point）に関連付けて QoS に活用します。ネットワーク間を流れる IP パケットはヘッダ部に DSCP フィールドを含み、そのデータがどんな優先順位のもと、どのようにネットワーク間で送出されるかを示しています。DSCP フィールドはローカルな管理により定義される 6 ビットの値です。Wi-Fi アライアンスは、WMM と DSCP 間の値のマッピングを定め、提案しています。

アクセスポイントは、自分を通過する全パケットの IP ヘッダ中の DSCP フィールドを照合します。アクセスポイントは DSCP フィールドの値に従って、パケットに送出の優先順位を付けて適したキューを割り当てます。本プロセスは管理者による QoS 設定の有無にかかわらず、自動的に実行されます。

データの種類によって異なるキューが関連付けられます。各キューおよび、それぞれに関連付ける優先順位、パラメータは以下の通りです。

- Data 0（音声）。最高優先度キュー、最小遅延。遅延に敏感な VoIP やストリーミングメディアなどのデータは自動的に本キューに送られます。
- Data 1（ビデオ）。高優先度キュー、最小遅延。遅延に敏感なビデオデータは自動的に本キューに送られます。
- Data 2（ベストエフォート）。中優先度キュー、中スループット・中遅延。一般的な IP データは本キューに送られます。
- Data 3（バックグラウンド）。最低優先度キュー、高スループット。高いスループットを要する大容量データや、遅延に敏感ではないデータは本キューに送られます（例 : FTP データなど）。

AP プロファイル中の QoS 設定を使用して、EDCA（Enhanced Distributed Channel Access）パラメータを設定し、各キューがアクセスポイントからクライアントに向けて送出される時、またはクライアントからアクセスポイントに向けて送出される時にどのように処理されるかを定義することができます。

無線トラフィックは以下の方向で流れます。

- アクセスポイントからクライアントへの下り方向
- クライアントからアクセスポイントへの上り方向
- アクセスポイントからネットワークへの上り方向
- ネットワークからアクセスポイントへの下り方向

WMM が有効状態の時は、D-Link 統合アクセスシステム上の QoS 設定は、上の 2 つの流れ、つまり「アクセスポイントからクライアントへの下り方向（AP EDCA パラメータ）」と「クライアントからアクセスポイントへの上り方向（Station EDCA パラメータ）」に対して作用します。

WMM が無効状態の時でも、「アクセスポイントからクライアントへの下り方向（AP EDCA パラメータ）」のいくつかのパラメータは設定可能です。

ネットワークとアクセスポイント間のトラフィックフローについては、アクセスポイント上での QoS 設定をサポートしていません。

データフレームの EDCF 制御と AIFS

データは 802.11 無線ネットワーク上をフレームの形で送信されます。フレームは連続したデータのある一部と記述的なメタ情報で構成されており、無線ネットワーク上で送受信するためにパッケージ化されています。

各フレームには、ソースアドレスと宛先 MAC アドレス、コントロールフィールドにプロトコルバージョン、フレームタイプ、フレームシーケンス番号、そしてフレームボディ（送信する実際の情報）およびエラー検出用のフレームチェックシーケンスが含まれます。

802.11 標準では、無線インフラストラクチャの管理・制御、およびデータ転送するために様々なフレームタイプを定義しています。それらは、（1）管理フレーム（2）制御フレーム、そして（3）データフレームです。無線インフラストラクチャの供給の管理・制御するための管理フレームと制御フレームの送出には、自動的に高い優先順位が与えられています。

802.11e では、Inter-frame Space（フレーム間の時間間隔）を使用することにより、どのフレームがチャンネルを獲得できるかの規定や、異なる種類のデータが送出されるまでの待ち時間を調整します。

管理・制御フレームの送出までの待ち時間（SIF: Short Inter-frame Space）は、最も短く定義されています。この値はインフラストラクチャサポート用として 802.11 によってはじめから定義されており、変更することはできません。

D-Link 統合アクセスシステムは、802.11e 標準で規定される EDCF（Enhanced Distribution Coordination Function）をサポートします。EDCF とは CSMA/CA プロトコルを用いる DCF を強化したもので、データフレーム間の Inter-frame Space（IFS）を定義しています。

データフレームの送出は、AIFS（Arbitration Inter-frame Space）として定義された時間待った後に行います。
本パラメータの値は指定可能です。

ランダムバックオフとコンテンション画面

メディアが使用中であることをアクセスポイントが検出すると、DCF ランダムバックオフタイマを使用して、チャンネルへのアクセスを再度トライするまでの待ち時間を決定します。各アクセスポイントで、リトライの間にランダムな時間待つことになります。待ち時間（初回は Minimum Contention Window で指定する値の幅の中からランダムな値）は、Maximum Contention Window で指定する値に到達するまで、指数関数的に増加していきます。そのようなランダムな待ち時間を設けることにより、複数のアクセスポイントが同時にデータの送信しようとメディアにアクセスを試みる際の衝突を回避することができます。ネットワーク上に活発なユーザの数が多くなるほど、バックオフタイマを利用して衝突や再送信の回数を減らすことによるパフォーマンスの向上は、より高く見込まれるようになります。

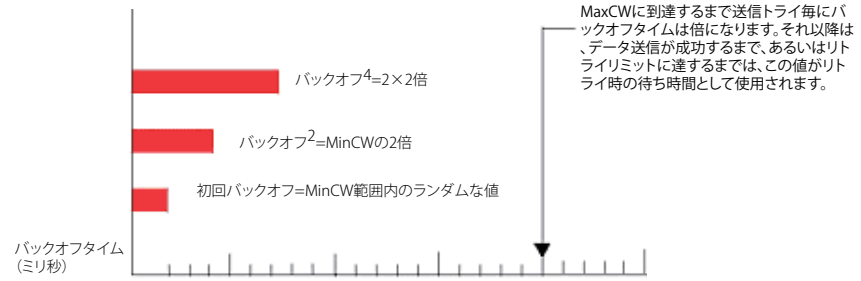


図 D-1　MTU サイズの入力

アクセスポイントで使用するランダムバックオフ値は指定可能なパラメータです。この待ち時間を指定するために、「Minimum Contention Window」（MinCW）と「Maximum Contention Window」（MaxCW）が定義されています。

- Minimum Contention Window に指定する値は、「初回ランダムバックオフ待ち時間」の範囲の上限として指定します。1 番目の待ち時間は、0 から Minimum Contention Window に指定する範囲でランダムに生成されます。
- データフレームが送信される前に、1 番目のランダムバックオフ待ち時間が終了すると、リトライカウンタは 1 増加し、ランダムバックオフ値（画面）は 2 倍の値になります。このランダムバックオフ値が、次のフィールドの cwMax で定義する値に到達するまで、またはデータ送信に成功するまで、終了に伴って値を倍にしていきます。

性能向上のためのパケットバースティング機能

D-Link の統合アクセスシステムは 802.11e 標準ベースのパケットバースティング技術を採用し、無線ネットワークでのデータのスループットと伝送スピードを向上させています。この機能を利用すると、余分なヘッダオーバヘッドを付加することなく、複数のパケットを連続送信できるようになります。これにより、ネットワークスピードとデータスループットを増強します。パケットバーストのサイズ（maximum burst length）はパラメータとして指定可能です。

クライアントの TXOP インターバル

TXOP（Transmission Opportunity: 送信権）は WMM（Wi-Fi Multimedia）クライアントが無線メディア（WM）に送信を開始する権利を持つ時間の間隔を意味します。

IEEE 802.1p 標準と DSCP タグ

IEEE 802.1p は IEEE 802 標準を強化した標準規格で、QoS 関連の規定をしています。802.1p 策定の 1 つの目的は、データリンク /MAC レイヤでのネットワークトラフィックの優先順位付けです。

802.1q タグは優先順位決定に使用される 3 ビットのフィールドを使用し、それによりパケットを様々なトラフィッククラスにグループ分けします。8 つの優先度レベルが定義可能です。最も優先度が高いクラスは 7、でネットワーククリティカルなトラフィック（音声）がこれに当てはまります。最も優先度が低いクラスは 0 で、ベストエフォート型のサービスに使用します。他に値が設定されなければ、この値が自動的に適用されます。

注意 IEEE 802.1p の優先度制御は、QoS と WMM が有効に設定されている時のみ行われます。WMM はアクセスポイントと、それに接続するクライアントの両方で有効である必要があります。

図 D-2 はタグが読み出され、ネットワークでのトラフィックの優先度を決定する方法について概説します。

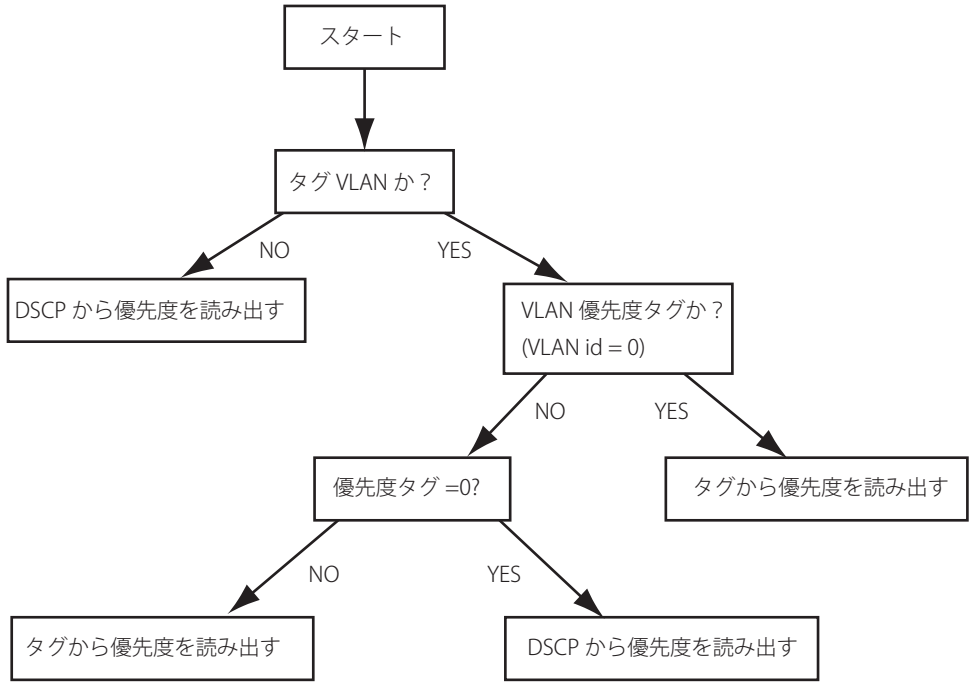


図 D-2　トラフィックの優先順位付け

表 D-1 は VLAN 優先度と DSCP 値の対応を示します。

表 D-1　VLAN 優先度タグ

VLAN 優先度	優先度	DSCP 値
0	ベストエフォート	0
1	バックグラウンド	16
2	バックグラウンド	8
3	ベストエフォート	24
4	ビデオ	32
5	ビデオ	40
6	音声	48
7	音声	56